*Journal of The Korea Institute of Information Security & Cryptology* ISSN 1598-3986(Print)
VOL.24, NO.4, Aug. 2014 ISSN 2288-2715(Online)
http://dx.doi.org/10.13089/JKIISC.2014.24.4.705

# 금융기관의 IT운영리스크 관점에서의 응용프로그램 구조에 관한 연구

조 성 철,† 남 초 이, 이 경 호‡
고려대학교 정보보호대학원

# A Study on Application Structure for IT Operational Risk in Financial Institute

Seong-Cheol Cho,† Cho-Yee Nam, Kyung-Ho Lee‡
Center for Information Security Technologies(CIST), Korea University

## 요 약

최근 금융기관의 리스크 관리 측면에서 운영리스크의 중요성이 점점 부각되고 있다. 특히 IT시스템 장애로 인한 금융서비스 중단의 경우는 고객 민원 및 이탈, 이익 감소 등의 결과로 이어질 수 있다. 따라서 금융기관에서는 IT 응용프로그램 장애 발생에 따른 영향을 최소화하기 위한 다양한 노력이 이루어지고 있다. 금융기관 IT시스템은 각 업무기능의 중복개발 배제 및 유지보수 효율성을 위해서 공통모듈을 사용하고 있다. 하지만 공통모듈에 장애가 발생하는 경우에는 해당 모듈을 사용하는 모든 업무가 영향을 받을 수 있는 리스크가 존재한다. 본 연구에서는 IT운영리스크 관점에서 리스크가 큰 공통모듈은 업무별로 분리하도록 하여 응용프로그램 장애에 따른 피해에 대응하고자 한다. 이를 위해서 공통모듈과 관련된 요인 변수의 분석을 진행하였고, 금융기관 IT운영리스크 감소를 위한 공통모듈 분리여부 판단 기준을 제안한다.

## ABSTRACT

Recently the importance of operational risk is gradually increasing in risk management of financial institute. Especially the service interruption caused by system failure can lead to customer complaints, decrease of profit and customer secession. Thus, financial industry makes diverse effort to minimize the impact caused by the system failure of IT application. Common modules are used in IT system in financial industry to exclude redundant development and to use the system efficiently. However, when a failure in common module is occurred, the risk that affects all the tasks using the common module exists. In this study, the damage affected by a failure in application program is prevented separating common module which has a large risk by task in the perspective of IT operational risk. In order to cope with damage, the research on the factors related to common module is conducted and proposes the separating common module standard for decrease of operational risk of the financial IT.

**Keywords:** risk management, IT operational risk, common module

접수일(2014년 5월 26일), 수정일(2014년 7월 9일), 게재확정일(2014년 7월 14일)

† 주저자, magiccsc@korea.ac.kr
‡ 교신저자, kevinlee@korea.ac.kr(Corresponding author)

# I. 서 론

## 1.1 연구배경 및 목적

금융기관의 업무처리 전반이 IT시스템에 의해 이루어지고 있는 상황에서 IT시스템의 장애, 정보의 유출, 테러와 같은 외부요인, 자연재해 등으로 인한 손실이 발생할 가능성이 증대되고 있다[1]. 특히 금융IT시스템의 장애로 인해 금융서비스가 중단되는 경우에 고객의 민원, 영업기회상실로 인한 영업이익감소, 고객이탈 등의 손실을 입게 된다. IT시스템에서 발생한 장애에 대응이 적절하게 취해지지 않으면, 장애복구시간에 비례하여 수익상실률이 10일 이내에 25%~50% 까지 감소된다고 한다[2].

IT시스템 장애에 대한 감독도 더욱 강화되고 있다. 금융감독원의 전자금융감독규정 제73조 정보기술부분 및 전자금융 사고보고에 대한 규정에는 금융회사 및 전자금융업자는 정보처리시스템 또는 통신회선 등의 장애로 10분 이상 전산업무가 중단 또는 지연된 경우, 전산자료 또는 프로그램의 조작과 관련된 금융사고가 발생한 경우, 전자적 침해행위로 인해 정보처리시스템에 사고가 발생하거나 이로 인해 이용자가 금전적 피해를 입었다고 금융회사 또는 전자금융업자에게 통지한 경우 등에는 지체 없이 금융위원회 및 금융감독원장에게 보고를 하도록 정하고 있다. 이러한 사고보고를 고의로 지연하거나 숨긴 자에 대해서는 소정절차에 따라 징계 등 필요한 조치를 취하여야 한다라고 명시하고 있다.

최근 금융기관의 손실 발생의 원인으로 운영리스크가 대두됨에 따라 운영리스크 관리의 중요성이 부각되고 있다. 금융 업계의 경우, 금융리스크에 대한 연구는 다양하게 진행되고 있으나[3], 금융IT시스템의 리스크 관리는 사후처리에 집중되고 있다[4]. 따라서 사전에 장애를 예방할 수 있는 방안에 대한 연구의 필요성이 증가하고 있다.

금융기관의 IT시스템에서 각 단위 시스템의 동일하거나 유사한 기능이 중복적으로 구현이 된다면 이로 인한 유지보수 시간과 비용이 지속적으로 증가하게 된다. 이를 해결하기 위하여 각 업무별로 분산되어 있는 기능을 공통화 하여, 중복 개발을 배제시키고 시스템의 효율적 사용 및 공통모듈의 재사용을 통해 업무개발의 생산성을 높일 수 있다. 하지만 공통모듈은 관련된 모든 업무에 영향을 미치기 때문에 장애 발생 시 파급효과가 크므로 리스크 측면을 고려해야 할 필요가 있다. 공통모듈 적용에 따른 리스크가 큰 경우에는 해당 모듈을 분리 적용하여 장애에 따른 피해를 감소시킬 수 있다.

본 논문에서는 각 공통모듈의 장애발생에 따른 리스크 크기에 영향을 미치는 요인 변수들을 도출하고 수집된 데이터를 통계적 기법으로 분석하여 IT운영리스크를 감소시키기 위한 공통모듈 구성하는 기준을 제안하고자 한다.

## 1.2 연구방법 및 구성

본 논문의 목적을 달성하기 위하여 운영리스크에 대한 문헌연구와 함께, A은행의 공통모듈 처리현황 데이터를 수집하였다.

본 논문의 구성은 다음과 같다.

서론에서는 연구배경 및 목적, 연구방법 및 구성 대해 기술하였고, Ⅱ장에서는 관련 연구로 운영리스크의 정의와 관련 연구를 고찰하였다. Ⅲ장에서는 연구대상인 공통모듈의 정의와 역할, 연구가설 및 연구 변수 설정하였으며 Ⅳ장에서는 각 요인 변수들 간의 상관관계를 분석하였다. 마지막으로 Ⅴ장에서는 결론을 맺으며 본 논문의 한계 및 향후 발전방향에 대해 기술하였다.

# II. 관련연구

## 2.1 운영리스크의 정의

BaselⅡ에서는 운영리스크를 협의로 정의하여 부적절하거나 잘못된 내부의 절차, 인력 및 시스템 또는 외부의 사건으로 인해 발생하는 손실리스크로 정의하며 법률리스크(legal risk)는 포함하지만, 전략리스크(strategic risk)와 평판리스크(reputational risk)는 제외하고 있다. 전략리스크와 평판리스크를 제외하는 것은 해당 리스크가 별도로 정의되는 리스크가 아니라 다른 운영리스크 손실사건에서 산출되는 개념이고 BaselⅡ가 규제자본을 산출하는 측면에서 계량적으로 파악 가능한 리스크만을 고려하기 때문인 것으로 볼 수 있다[1].

김종호는 금융기관의 리스크관리가 시장리스크(market risk)와 신용리스크(credit risk)의 측정 및 관리보다 최근에는 운영리스크(operational risk) 관리가 중요하게 대두되고 있다고 하면서, 운영리스크는 협의의 정의에서는 거래처리(transaction processing)에 한정되지만, 광의의 정의에서는 신용

리스크나 시장리스크를 제외한 모든 재무적 리스크를 모두 운영리스크로 정의하고 있다고 보았다[5].

BBA(British Banker's Association)가 제시한 운영리스크의 정의에서는 내부리스크(internal risk)와 외부리스크(external risk)가 포함되어 있는데 내부리스크에는 인적리스크, 프로세스리스크, 기술리스크가, 외부리스크에는 외부리스크, 물리적 리스크가 포함되어 있다. 이 중 기술리스크는 시스템, 프로그램, 데이터에 의해 발생하는 운영리스크를 의미하며, 자료의 질이나 프로그램상의 오류, 시스템 부적합성에 따른 오류 등이 포함된다[5].

Table 1. The definition of operational risk(BBA)

| | | |
|---|---|---|
| Internal risk | People risk | Conspiracy of employees, fraud, absence of knowledge, Leaving of core manpower |
| | Process risk | Accounting errors, Product complexity, Billing and payment errors, Valuation errors |
| | Technology risk | The quality of the data, An error in the program, Inadequacies of the system |
| External risk | External risk | Legal risk, Regulatory risk, Outsourcing risk, Supplier Risk |
| | Physical risk | Fire, Natural disasters, Theft |

양영찬은 전통적으로 운영리스크(operational risk)는 신용리스크, 시장리스크, 금리리스크, 유동성리스크 등과 같은 여타 금융리스크를 제외한 모든 리스크로 광의로 정의된다고 하였다[6].

임경진은 운영리스크는 부분적으로 기술리스크와 연관되어 있는 것으로 기존의 기술이 잘못 작동하거나 백오피스 지원시스템이 망가질 때 발생한다고 하였다. 즉 운영리스크는 부적절한 내부시스템, 관리실패, 잘못된 통제, 사기, 인간의 오류 등을 포함한다. 운영리스크는 거래가 실행되지 못하는 데에서 발생하는 실행리스크(execution risk), 시스템의 무단침입, 변경과 같은 기술리스크(technology risk), 그리고 잘못된 모형을 사용하여 가치를 평가하는 데에서 발생하는 모형리스크(model risk) 등을 포함한다고 하였다[7].

## 2.2 운영리스크의 특징

운영리스크는 시장리스크 및 신용리스크와 다른 특징을 보인다. 첫째, 시장리스크, 신용리스크는 금융기관의 수익과 직접적으로 관련되는 반면, 운영리스크는 영업활동에 내재되어 있으며, 수익과 간접적인 관계를 갖고 있다. 둘째, 시장리스크, 신용리스크와는 달리 운영리스크는 금융기관의 전 영업활동을 포괄하므로 사람, 프로세스, 시스템에 내재되어 있어 구체적인 익스포저(위험노출액)를 파악하는 것이 어렵기 때문에 주관적인 방법을 사용하게 되어 객관성이 떨어지게 된다. 셋째, 운영리스크는 금융기관 전체를 통해 내부감사, 준법감시인, 운영리스크 관리팀 등 복수기관의 협력이 중요하며 전사적인 관심이 요구된다. 넷째, 운영리스크는 손실자료 부족으로 인해 실질적으로 측정하기가 매우 어렵다[8]. 현재 우리나라에서는 운영리스크와 관련된 손실자료의 표준화 및 보안을 보장하고 손실자료의 양적 부족을 보충하기 위해서 운영리스크 손실자료 공유 위원회 KOREC(Korea Operational Riskdata Exchange Committee)를 2006년에 구성하였으며, 현재 6개 은행이 KOREC에 가입되어 있다. KOREC 회원은행은 3개월마다 손실자료 관리기관인 은행연합회에 손실자료를 제출하고 있으며, 은행연합회는 통합손실자료 및 보고서를 회원은행에 제공하고 있다.

Table 2. Comparison on market risk, credit risk, operational risk[9]

| Sector | Market risk | Credit risk | Operational risk |
|---|---|---|---|
| Exposure | Real assets such as marketable assets, moan assets | | Human resource, business processes, and business characteristics |
| Cause of Lost | Market | | Human resource, internal processes, and culture |
| Related depart-ments | Asset management department | Loans department | All departments |

| | | | |
|---|---|---|---|
| Risk awareness | Objective data to identify increased market volatility, increased exposure, etc. | | Risk & Control Self-Assessment |
| Manage-ment authority | Market risk team (Single authority) | Credit risk team (single authority) | Internal Audit / Compliance Officer / Operational Risk Management Team (plural authority) |
| Loss distribut-ion | Normal | Skewed Distribution (Beta, Gamma) | Skewed Distribution (Frequency distribution, loss distribution) |
| Event | Increase market volatility | Bankruptcy | Operating loss(More rare bankruptcy case) |
| Number of loss events | Countless | Plenty | Worldwide shortage |

## 2.3 운영리스크의 주요 발생 원인과 중요성

운영리스크의 주요 발생 원인은 내부프로세스와 인적리스크, 시스템리스크, 외부리스크 등으로 나누어 볼 수 있으며 부적절한 프로세스와 인적 통제로 인하여 사기, 횡령 등이 유발될 수 있으며 시스템과 외부요인에 의해 시스템 장애 및 사기 등이 발생될 수 있다[10]. 이러한 원인들에 의해 발생되는 운영리스크은 대부분 시장리스크 또는 신용리스크과 결합되어 발생하는 경우가 많다[5].

한편 금융기관의 업무처리가 IT시스템에 의존하기 때문에 IT시스템의 장애 등 시스템에 의한 손실의 가능성이 증대되고 있다. 또한 이러한 내부적인 요인에 의한 손실뿐만 아니라 외부적인 요인들에 의한 손실도 증가하고 있는 추세이다[10].

Table 3. Failures of operational risk management[5]

| Financial institution | Losses | Summary |
|---|---|---|
| Barings bank | $1.4 billion | Nicholas Leeson, a former derivatives broker in Barings bank, bankrupted the bank by fraudulent and unauthorized speculative trading causing the loss of $1.4 billion. |
| Daiwa bank | $1.1 billion | Toshihide Iguchi, a former executive VP and U.S. Government Bond trader at Daiwa Bank's New York Branch, caused the loss of $1.1 billion. |
| Sumitomo bank | $2,600,000 | A Copper trader unreported the loss for three years causing the tarnishment of the bank's reputation. |
| Deutsch Morgan Grenfell | $720 million | A fund manager in Doichi bank exceeded the maximum limit causing the extensive loss. Doichi bank compensated the fund investors |
| Bankers Trust | $150 million | An inappropriate sales practice caused legal lawsuit and tarnished the bank's reputation |
| Natwest | $120 million | A swab trader inputted incorrect volatility into option pricing model causing the tarnishment of the bank's reputation. |

## 2.4 운영리스크 측정방법

운영리스크의 측정방법으로는 기초지표법(basic indicator approach), 표준방법(standardized approach), 고급측정법(advanced measurement approach)이 있다. 국제적으로 영업을 하고 있는 은행과 중요한 운영리스크에 노출된 은행은 고급측정법 사용을 권고하고 있다[11].

Table 4. Comparison on BIS regulatory and operational risk measurement [12]

| Management tasks | BIA | SA | AMA |
|---|---|---|---|
| Pillar 1<br><br>Minimum capital require-ments | Without condition. All banks should be satisfied but BIA is not apply to big bank but to small bank mainly. | Banks should satisfy the following requirements at least.<br>-Independent monitoring function. Supervising and recording about operating loss constantly. A valuation function<br>-Sales part are categorized according to the guideline.<br>-Need for a independent operating risk management organization for valuating and managing operational risk | Add the following conditions to previous one.<br>Approval of the operational risk data and model. The loss date for management risk should be available to check and use for a certain period of time<br>An elaborate model and skilled management organization for operational risk |
| Pillar 2<br><br>Supervision | Supervision Authorities inspect the management system for operational risk | Supervision Authorities inspect mapping of risk and loss of sales line and management of it | Supervision Authorities inspect operational risk and loss data |
| Pillar 3<br><br>Market discipline | Publicized the goal of capital adequacy ratio which is standard for managing risk management and ratio of equity capital which costs among total capital | Add exposure public managing risk according to sales department | Publicized a total among of the loss of managing risk according to sales department during a period |

다른 한편으로는 측정하는 접근 방식에 따라 하향식(top-down)과 상향식(bottom-up) 방식이 있다.

하향식 접근방법에서는 운영리스크가 개별사건 또는 손실의 원인에 대한 분석 없이 거시적인 자료에 의해 추정된다. 금융기관의 특성을 대변하는 경영지표(자산규모, 수익, 비용, 주가)를 이용하여 리스크량을 산출하는 방법이다. 이 방법은 리스크 산출방법이 비교적 간단하며 모든 금융기관에 대해 일률적인 방법을 적용할 수 있다. 그러나 리스크산출에 사용된 지표의 타당성에 대한 반론이 제기될 수 있으며 리스크의 원인 파악이 어려워 리스크에 관련된 책임소재가 불분명해지는 단점이 있다.

상향식 접근방법은 운영리스크의 규모와 원인을 알아보기 위해 개별사건들을 이용하며 금융기관의 모든 업무프로세스를 분석하여 업무와 관련된 모든 리스크를 자체 평가하고 합산하여 기업 전체의 리스크량을 산출하는 방법이다. 이는 정성적 관리기법과 상호보완적으로 사용이 가능하며 리스크 원인 파악이 용이하다. 또한 시장리스크와 신용리스크에서 활용된 계량화 기법을 응용할 수 있다. 단점으로는 손실데이터 정비에 많은 시간과 인력이 필요하다는 점이 있다[13].

### 2.5 IT운영리스크 관련 연구

운영리스크에 관한 연구 중 IT운영리스크와 관련된 선행연구를 Table 5.에 정리하였다. 선행연구에서는 IT운영리스크 관리방안으로 통합 리스크 관리시스템, 장애모형, 감리모형 등을 제안하고 있다.

Table 5. Preceding studies on IT operational risk

| Researcher | Summary |
|---|---|
| Hyun-ju Shin, 1999 | Suggested that solution of risk management problem in financial institute is building risk management system which is appropriate in our financial environment and database for risk management |
| Yong-sub | To build the Business Recovery |

| | |
|---|---|
| Kim, 2002 | System for financial institution, the recovery plan for primary computer center's function considering implementation technology, the scale of system, communication methods, and communication line is suggested. |
| Seung-mi Hong, 2002 | For successful risk management in domestic bank, the integrated risk management system to exactly assess and manage the risk and the regulation for risk management including exact responsibilities and reporting system should be operated. |
| Young-gon Kim, 2003 | analyzed the type of operational risk and in order to reduce operational risk, the checklist for division, transfer checking program, improvement of labor conditions to harmonize with subsidiary companies or service employees, standardized job descriptions and operational guideline for each division updated periodically, systematically construction of backup center, system expansion for preventing interruption of operation, intrusion prevention program for hacking, etc are suggested. |
| Young-joun Youn, 2005 | In study for risk factors of IT project in financial institution, communication, schedule, plan, project management, technology, requirement/range, relation management, user resistance, capital, company's environment, support from board of directors were suggested as risk factors. |
| Young-Jai Lee, 2007 | Prevention and preparation are required to minimize IT operational risk and to reduce the loss from system failure. To do this, failure preventing variables to predict and minimize possible failure are the cause of failure, inspection interval, and operation provision. |
| Young-chan Yang, 2009 | To reduce operational risk, operational risk management through IT system is important. Operational risk supervision model to satisfy the level required by the Financial Supervisory Authority and to let the third party systematically and consistently perform operational risk inspection is deducted. |
| Dong-jin Park, 2011 | The loss from operational risk is greater than other risk and operational risk affects future competition in financial institution. Building operational risk system to exactly assess risk and establishing assessment standard are required. |

### 2.6 선행 연구와의 차이점

본 논문은 첫째, 기존의 연구에서 다루지 않았던 IT시스템의 전 영역에서 공통으로 사용되고 있는 응용 프로그램의 관점에서 IT운영리스크를 감소시킬 수 있는 방안을 찾기 위해 수행되었다. 둘째, 새로운 시스템 및 규정의 개발 없이 현재 시스템을 분석하여 바로 적용이 가능하다. 셋째, 연구의 관점이 장애 발생 이후의 대책이 아닌 사전에 장애에 따른 영향을 줄이기 위한 방안을 제시한다는 점에서 차이가 있다.

## III. 연구대상 및 가설 설정

### 3.1 공통모듈의 정의와 종류

자료 수집 및 연구의 대상이 되는 A은행의 공통모듈은 IT시스템 전체에 영향을 미치는 서비스를 제공한다. 공통모듈은 공통적인 기능과 공통 프로세스에 의하여 수집된 데이터를 공통모듈을 통하여 업무팀에서 사용할 수 있도록 제공하며, 유지보수시 생산적이고 효율적이라고 판단되는 기능을 중심으로 선정된다.

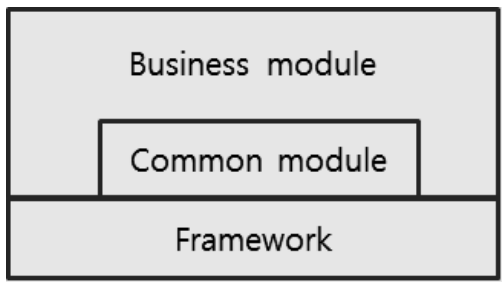


Fig. 1. The scope of common module

Table 6. The list of common module

| Sector | Common module |
|---|---|
| Generate support | Account number generation |
| | Control number generation |
| | Password restriction check |
| | Customer designated account number generation |
| | Number generation for card interface |
| Information support | Currency code inquiry |
| | Exchange rate inquiry |
| | Commodity futures exchange inquiry |
| | Bill clearance time inquiry |
| | Branch information inquiry |
| | Integrated branch inquiry |
| | Branch support history inquiry |
| | Bank instance code inquiry |
| | Bank instance code multiple inquiry |
| | Error message code, Officer approve reason code, Action message code inquiry |
| | Employee information inquiry |
| | Business day inquiry/change |
| | Tax information inquiry |
| | Country list inquiry |
| | Bank List inquiry |
| | Bank code inquiry |
| | User rights and Sales/OP information inquiry |
| | Transaction control information inquiry |
| | Existence of an instance code inquiry |
| | Inquiry whether the VIP lounge |
| | Employee existence inquiry |
| | Real name token images key store and inquire |
| Computation support | Number of days/months/business days/holidays calculation |
| | Calculate the number of days(subtracting entered number of months) |
| | Expiration date calculation |
| | Date interval calculation |
| | Time calculation |
| | beginning of the month/end of the month calculation |
| | Age calculation |
| | Leap year check |
| | Holiday check |
| | Business day calculation |
| | Date calculation |
| | Beginning of business day, end of business day calculation(month) |
| | Gregorian/lunar date conversion |
| | Date validation check |
| | Day of the week calculation |
| | Account number check digit generation and verification |
| | M/S check digit generation and verification |
| | General check digit validation |
| | Control number check digit generation and verification |
| | End of the month calculation |
| | Business day calculation II |
| | Date calculation II |
| | Stock exchange holiday/expiration date calculation |
| | Officer approve reason check |
| | EBCDIC Hangul code verification |
| | Electronic public slip check rule |
| Conversion support | Date Conversion(year, month, week) |
| | Date Conversion(year, month, day of the week) |
| | Old account number conversion |
| | Account number conversion(using algorithm) |
| | String length conversion |
| | Stated number Hangul/English conversion |
| | Variable-length data conversion |
| | Conversion for privacy |
| | Image recognition code encryption |
| | Combining the separated data |
| | External organizations standard error message code, action message code inquiry |
| | Remove the data space |
| | Slip number generation |
| | Real name token images key restore |

### 3.2 연구가설 및 연구변수 설정

본 논문에서는 공통모듈 적용에 따른 리스크에 영향을 미치는 변수의 선정시 기존 연구에서는 참고할 자료가 없어서 전문가 의견을 바탕으로 도출하였고, 각 변수들이 리스크의 크기에 영향을 주는 정도가 다를 수 있다는 가정 하에 분석을 수행하였다.

설문조사는 IT운영리스크에 많은 영향을 미치는 요인 변수를 채택하기 위하여 실시하였으며 5점 척도를 사용하여 관련도에 따라 1~5점으로 구성하였다. 자료 수집은 금융기관의 관련 업무에 경력이 10년 이상인 전문가 30명을 대상으로 인터뷰 및 e-mail에 의한 방법을 사용하였다.

Table 7. Factors affecting IT operational risk

| Factor variables | Score | % |
|---|---|---|
| The number of programs calling common module | 145 | 11% |
| The number of tasks associated with common module | 139 | 10% |
| The frequency of using common module | 141 | 10% |
| Transaction medium that calling common module | 114 | 8% |
| The number of incident occurred that caused by common module | 148 | 11% |
| Change cycle of the common module | 118 | 9% |
| The transaction time that common module intensive processing | 89 | 7% |
| Difficulty developing a common module | 109 | 8% |
| Common module developer's skills | 97 | 7% |
| The number of transaction code calling common module | 137 | 10% |
| The period for developing common module | 118 | 9% |
| Total | 1355 | 100% |

설문조사를 통하여 얻은 결과에서 관련도가 높은 상위 5개를 요인 변수로 채택하였으며, 공통모듈 적용에 따른 리스크는 호출 프로그램 수, 연관 업무 수, 사용빈도수, 인시던트 발생회수, 거래코드수와 상관관계가 있으며, 리스크의 크기는 거래금액과 비례한다고 가정하였다.

H1: 공통모듈을 호출하는 프로그램수와 거래금액은 상관관계가 있다.
H2: 공통모듈과 관련된 연관 업무 수와 거래금액은 상관관계가 있다.
H3: 공통모듈이 호출되는 사용빈도수와 거래금액은 상관관계가 있다.
H4: 공통모듈이 원인이 되어 발생한 인시던트 발생회수와 거래금액은 상관관계가 있다.
H5: 공통모듈을 호출하는 거래코드수와 거래금액은 상관관계가 있다.

### 3.3 자료수집 및 분석방법

연구를 위한 자료는 A은행의 최근 1년 동안의 공통모듈 사용과 관련한 거래금액, 사용빈도수, 인시던트 발생회수와 프로그램, 연관업무 및 거래코드 데이터를 수집하였다. 수집한 데이터의 상관도 분석 및 산점도는 SPSS 21(Statistical Packages for Social System)을 사용하였으며 상관분석시 적용된 상관계수는 Pearson 상관계수이다.

## IV. 분석 결과

### 4.1 상관분석 및 결정 모델 도출

첫 번째로 호출 프로그램 수와 거래금액과의 상관분석 결과는 다음과 같다.

Table 8. Correlation analysis between the number of calling programs and the transaction amount

**Descriptive statistics quantity**

| | Average | Standard deviation | N |
|---|---|---|---|
| Number of calling programs | 620.54 | 1046.661 | 67 |
| Transaction amount | 8972416727931430.00 | 8148086254193950.000 | 67 |

**Correlation coefficient**

| | | Number of calling programs | Transaction amount |
|---|---|---|---|
| Number of calling programs | Pearson correlation coefficient | 1 | .441** |
| | significance probability | | .000 |
| | N | 67 | 67 |
| Transaction amount | Pearson correlation coefficient | .441** | 1 |
| | significance probability | .000 | |
| | N | 67 | 67 |

**. 상관계수는 0.01 수준(양쪽)에서 유의합니다.

호출 프로그램 수와 거래금액의 상관계수는 0.441로 유의수준 0.001에서 귀무가설은 기각되며 연구가설은 지지된다. 즉, 호출 프로그램 수는 거래금액과 상관관계(+)가 있다고 할 수 있다.

두 번째로 연관 업무 수와 거래금액과의 상관분석 결과는 다음과 같다.

Table 9. Correlation analysis between the number of tasks associated with and the transaction amount

**Descriptive statistics quantity**

| | Average | Standard deviation | N |
|---|---|---|---|
| Number of tasks associated | 22,03 | 16,525 | 67 |
| Transaction amount | 8972416727931430,00 | 8148086254193950,000 | 67 |

**Correlation coefficient**

| | | Number of tasks associated | Transaction amount |
|---|---|---|---|
| Number of tasks associated | Pearson correlation coefficient | 1 | ,517** |
| | significance probability | | ,000 |
| | N | 67 | 67 |
| Transaction amount | Pearson correlation coefficient | ,517** | 1 |
| | significance probability | ,000 | |
| | N | 67 | 67 |

**, 상관계수는 0,01 수준(양쪽)에서 유의합니다.

연관업무수와 거래금액의 상관계수는 0.517로 유의수준 0.001에서 귀무가설은 기각되며 연구가설은 지지된다. 즉, 연관업무수는 거래금액과 상관관계(+)가 있다고 할 수 있다.

세 번째로 사용빈도수와 거래금액과의 상관분석 결과는 다음과 같다.

Table 10. Correlation analysis between frequency of use and the transaction amount

**Descriptive statistics quantity**

| | Average | Standard deviation | N |
|---|---|---|---|
| Frequency of use | 3113808250,75 | 3799958520,372 | 67 |
| Transaction | 8972416727931430,00 | 8148086254193950,000 | 67 |

**Correlation coefficient**

| | | Frequency of use | Transaction amount |
|---|---|---|---|
| Frequency of use | Pearson correlation coefficient | 1 | ,700** |
| | significance probability | | ,000 |
| | N | 67 | 67 |
| Transaction amount | Pearson correlation coefficient | ,700** | 1 |
| | significance probability | ,000 | |
| | N | 67 | 67 |

**, 상관계수는 0,01 수준(양쪽)에서 유의합니다.

사용빈도수와 거래금액의 상관계수는 0.700로 유의수준 0.001에서 귀무가설은 기각되며 연구가설은 지지된다. 즉, 연관 업무 수는 거래금액과 상관관계(+)가 있다고 할 수 있다.

네 번째로 인시던트 발생회수와 거래금액과의 상관분석 결과는 다음과 같다.

Table 11. Correlation analysis between the number of incident occurred and the transaction amount

**Descriptive statistics quantity**

| | Average | Standard deviation | N |
|---|---|---|---|
| Number of incident occurred | ,30 | 2,082 | 67 |
| Transaction amount | 8972416727931430,00 | 8148086254193950,000 | 67 |

**Correlation coefficient**

| | | Number of incident occurred | Transaction amount |
|---|---|---|---|
| Number of incident occurred | Pearson correlation coefficient | 1 | ,161 |
| | significance probability | | ,194 |
| | N | 67 | 67 |
| Transaction amount | Pearson correlation coefficient | ,161 | 1 |
| | significance probability | ,194 | |
| | N | 67 | 67 |

인시던트 발생회수와 거래금액의 상관계수는 0.161이며 유의 확률이 0.194로 유의수준 .001에서 귀무가설은 지지된다. 즉 거래금액은 인시던트 발생회수와 상관관계가 없다고 할 수 있다.

다음으로 거래코드수와 거래금액과의 상관분석 결과는 다음과 같다.

Table 12. Correlation analysis between the number of transaction code and the transaction amount

**Descriptive statistics quantity**

| | Average | Standard deviation | N |
|---|---|---|---|
| Number of transaction code | 142,58 | 146,582 | 67 |
| Transaction amount | 8972416727931430,00 | 8148086254193950,000 | 67 |

**Correlation coefficient**

| | | Number of transaction code | Transaction amount |
|---|---|---|---|
| Number of transaction code | Pearson correlation coefficient | 1 | ,766** |
| | significance probability | | ,000 |
| | N | 67 | 67 |
| Transaction amount | Pearson correlation coefficient | ,766** | 1 |
| | significance probability | ,000 | |
| | N | 67 | 67 |

**, 상관계수는 0,01 수준(양쪽)에서 유의합니다.

거래코드수와 거래금액의 상관계수는 0.766로 유의수준 0.001에서 귀무가설은 기각되며 연구가설은 지지된다. 즉, 연관 업무 수는 거래금액과 상관관계(+)가 있다고 할 수 있다.

분석 결과를 살펴보면 인시던트 발생회수를 제외한 각 변수와 리스크의 크기가 상관관계가 있음을 알 수

있다. 거래코드수, 사용빈도수, 연관 업무 수, 호출프로그램 순으로 상관도가 크므로 공통모듈 분리여부 결정시 가중치 부여가 가능하며 이를 이용하여 IT공통모듈 구성을 위한 절차를 구성하면 Fig.2와 같다.

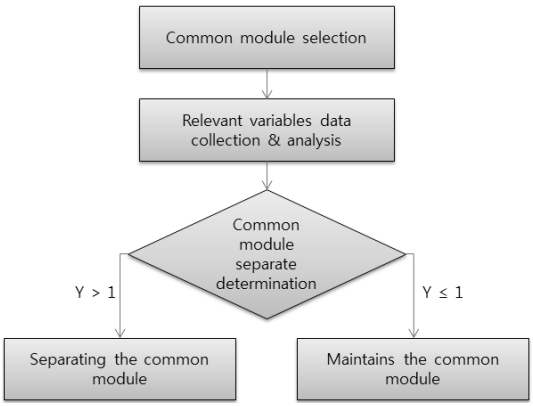


Fig. 2. The procedure for common module separation decision

공통모듈 분리여부 판단을 위한 기준은 상관분석의 결과인 상관계수의 크기를 가중치로 사용하여 나타내면 Table 13.과 같다.

Table 13. The formula for common module separation decision

$Y=0.766X_1 + 0.7X_2 + 0.517X_3 + 0.441X_4 + C$

$Y$ : Standard for separating common module (Y〉1 : Separate, Y≦1 : Maintain)
$X_1$ : The number of transaction code
$X_2$ : Frequency of use (1 hour average)
$X_3$ : The number of tasks associated with
$X_4$ : The number of programs
$C$ : constant (-600,000)

### 4.2 산점도를 통한 검증

제안한 분리여부 판단 식에 대한 검증을 위해 각 변수에 대한 산점도에서의 리스크 크기와 계산 결과를 비교하였다.

Fig.3.은 변수와 거래금액의 산점도 위치에 따른 리스크의 크기를 고위험(High), 중위험(Medium), 저위험(Low)으로 나타낸 것이고, Fig.4.~Fig.7.은 산점도이다.

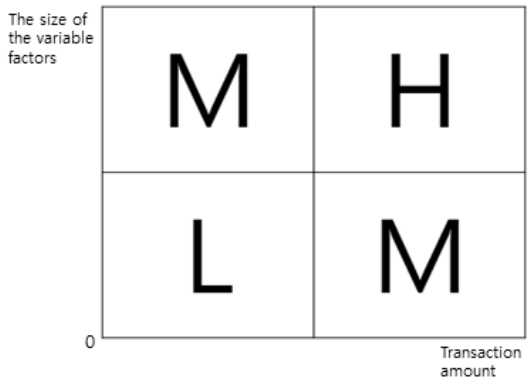


Fig. 3. The size of the risk

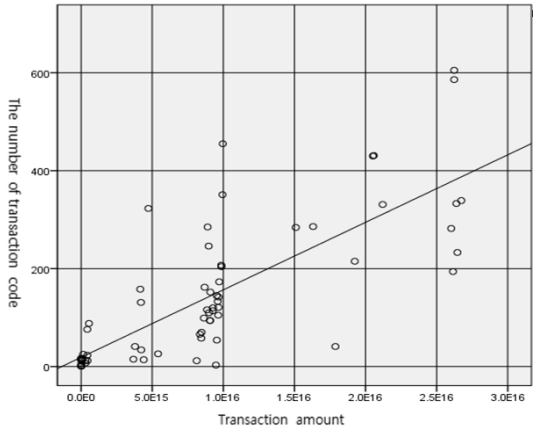


Fig. 4. A scatter plot of the number of transaction code and the transaction amount

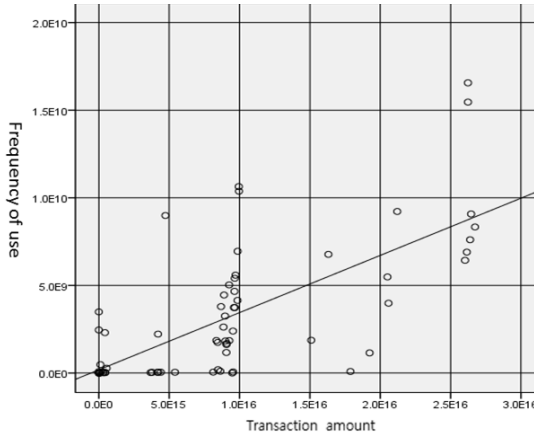


Fig. 5. A scatter plot of frequency of use and the transaction amount

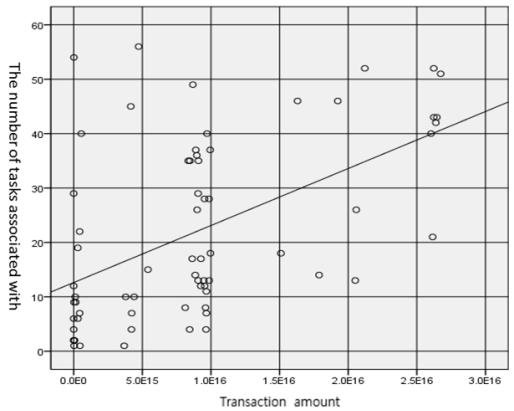


Fig. 6. A scatter plot of the number of tasks associated with and the transaction amount

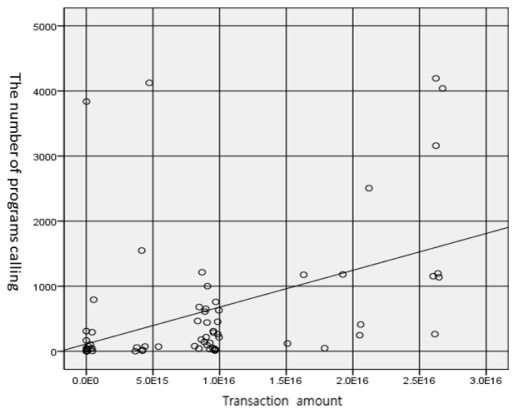


Fig. 7. A scatter plot of the number of programs calling and the transaction amount

Table 14.의 A열은 변수가 거래코드수인 경우의 리스크 크기를 나타내며, B열은 사용빈도수, C열은 연관 업무 수, D열은 호출 프로그램수인 경우의 리스크 크기이다. E열은 해당 공통모듈에 대해서 수집된 데이터를 제안한 식에 적용하여 계산한 결과이며 계산 결과가 1보다 큰 경우에 Yes(분리대상), 1보다 작거나 같은 경우에는 No(유지대상)로 표시하였다. 마지막으로 F열에는 계산된 분리여부 판단 결과가 적정한지 검증하였다. 검증한 결과 각 공통모듈의 리스크의 크기가 고위험(H)이거나 중위험(M)이 2개 이상인 경우를 분리 대상으로 하였을 때, 전체 67개의 공통모듈 중 58개가 제안한 식의 결과와 일치함을 확인할 수 있었다.

Table 14. The result of applying the formula

| Common module | A | B | C | D | E | F |
|---|---|---|---|---|---|---|
| Account number generation | L | L | L | L | No | ○ |
| Control number generation | L | L | L | L | No | ○ |
| Password restriction check | L | L | L | L | No | ○ |
| Currency code inquiry | M | M | M | M | Yes | ○ |
| Exchange rate inquiry | L | L | M | L | No | ○ |
| Commodity futures exchange inquiry | L | L | L | L | No | ○ |
| Bill clearance time inquiry | L | L | L | L | Yes | × |
| Branch information inquiry | L | L | M | M | Yes | ○ |
| Integrated branch inquiry | L | M | M | L | Yes | ○ |
| Branch support history inquiry | L | L | L | L | No | ○ |
| Bank instance code inquiry | H | H | H | H | Yes | ○ |
| Bank instance code multiple inquiry | L | L | L | L | No | ○ |
| Error message code, Officer approve reason code, Action message code inquiry | L | L | L | L | No | ○ |
| Employee information inquiry | M | M | H | M | No | × |
| Business day inquiry/change | L | L | L | L | No | ○ |
| Number of days/months/business days/holidays calculation | M | M | H | M | Yes | ○ |
| Calculate the number of days(subtracting entered number of months) | L | L | L | L | No | ○ |
| Expiration date calculation | L | L | M | M | No | × |
| Date interval calculation | L | L | M | L | No | ○ |
| Time calculation | L | L | L | L | Yes | × |
| beginning of the month/end of the month calculation | L | L | M | L | No | ○ |
| Age calculation | M | M | L | M | No | × |

| | | | | | | |
|---|---|---|---|---|---|---|
| Leap year check | L | L | L | L | No | ○ |
| Holiday check | M | M | H | H | Yes | ○ |
| Business day calculation | L | L | M | L | No | ○ |
| Date calculation | L | L | M | L | No | ○ |
| Beginning of business day, end of business day calculation (month) | L | L | M | L | Yes | × |
| Gregorian/lunar date conversion | L | L | L | L | No | ○ |
| Date validation check | M | M | H | H | Yes | ○ |
| Day of the week calculation | L | L | L | L | No | ○ |
| Date Conversion (year, month, week) | L | L | L | L | No | ○ |
| Tax information inquiry | L | L | L | L | No | ○ |
| Old account number conversion | L | L | M | L | No | ○ |
| Account number conversion(using algorithm) | L | L | L | L | No | ○ |
| String length conversion | H | H | H | H | Yes | ○ |
| Stated number Hangul/English conversion | M | M | M | M | No | × |
| Variable-length data conversion | H | M | M | M | Yes | ○ |
| Conversion for privacy | L | L | L | L | No | ○ |
| Account number check digit generation and verification | L | L | L | L | No | ○ |
| M/S check digit generation and verification | L | L | L | L | No | ○ |
| General check digit validation | L | L | L | L | No | ○ |
| Control number check digit generation and verification | L | L | L | L | No | ○ |
| Country list inquiry | M | M | L | L | Yes | ○ |
| Bank List inquiry | L | L | L | L | No | ○ |
| Bank code inquiry | L | L | L | L | No | ○ |
| User rights and Sales/OP information inquiry | L | L | L | L | No | ○ |

| | | | | | | |
|---|---|---|---|---|---|---|
| Customer designated account number generation | L | L | L | L | No | ○ |
| Transaction control information inquiry | L | L | L | L | No | ○ |
| Image recognition code encryption | H | M | M | M | No | × |
| Officer approve reason check | M | M | H | M | Yes | ○ |
| EBCDIC Hangul code verification | L | L | L | L | No | ○ |
| Combining the separated data | L | L | L | L | No | ○ |
| External organizations standard error message code, action message code inquiry | L | L | L | L | No | ○ |
| Remove the data space | L | L | L | L | No | ○ |
| Slip number generation | M | M | H | M | Yes | ○ |
| End of the month calculation | L | L | L | L | No | ○ |
| Business day calculation II | M | M | H | M | Yes | ○ |
| Date calculation II | L | L | M | L | No | ○ |
| Stock exchange holiday/expiration date calculation | L | L | L | L | No | ○ |
| Date Conversion (year, month, day of the week) | L | L | L | L | No | ○ |
| Existence of an instance code inquiry | L | L | L | L | Yes | × |
| Inquiry whether the VIP lounge | L | L | L | L | No | ○ |
| Employee existence inquiry | L | L | L | L | No | ○ |
| Real name token images key store and inquire | L | L | L | L | No | ○ |
| Real name token images key restore | L | L | L | L | No | ○ |
| Electronic public slip check rule | L | L | L | L | No | ○ |
| Number generation for card interface | L | L | L | L | No | ○ |

검증과정에서 불일치가 발생한 모듈을 살펴보면, 중위험(M)이 1개 이하로 유지대상이지만 계산결과는 Yes(분리대상)으로 나온 경우는 해당 모듈의 요인 변수값은 크지만 거래금액이 작은 경우이었고, 중위험 이상이 2개이지만 No(유지대상)으로 나온 경우는 해당 모듈의 각 요인 변수의 크기는 작으나 거래금액은 큰 경우에 해당했다. 이러한 결과는 분리 기준식을 산점도에서의 리스크 크기를 통해 검증한 분석방법에 기인한다고 볼 수 있다.

## V. 결론 및 향후 발전방향

### 5.1 결론

금융기관의 운영리스크가 중요한 문제가 되고 있고 이에 따른 관리 방안이 여러 방면으로 연구되고 있다. 특히 IT시스템의 장애발생의 가능성이 증가함으로 인한 금융기관의 운영리스크를 관리하기 위해서는 IT운영리스크의 관리가 매우 중요하다.

본 논문에서는 금융기관 IT시스템의 응용프로그램 구조를 통해 IT운영리스크를 감소시킬 수 있는 방안을 연구하였다. 여러 업무팀에서 사용되어지는 공통모듈의 경우 장애가 발생했을 경우에 해당 모듈을 사용하는 모든 업무가 중단되는 리스크를 가지고 있다. 이러한 리스크를 감소시키기 위한 방안으로 공통모듈 중에서 리스크가 큰 모듈은 분리하여 적용하는 것을 고려할 수 있으며, 분리대상을 선정하는 기준을 도출하기 위한 연구를 진행하였다.

리스크 크기에 영향을 주는 요인이 되는 변수를 설문조사를 통해 채택하였고, 해당 변수에 관련한 데이터를 수집하여 통계적으로 상관분석을 수행하였다. 그 결과 거래코드수, 사용빈도수, 연관 업무 수, 호출 프로그램 수 순으로 리스크의 크기와 상관관계가 있음을 확인할 수 있었다. 해당 변수들은 공통모듈에 대한 IT운영리스크의 측정 지표로 사용될 수 있으며, 각 변수에 가중치를 적용함으로써 금융기관의 공통모듈 분리 여부 판단을 위한 기준을 제안하였다. 제안한 기준을 산점도를 이용해 검증한 결과 86.5%로 부합됨을 확인할 수 있었다.

본 논문에서 진행한 분석방법과 제안된 분리 기준은 각 금융기관에서 IT운영리스크를 감소를 위한 방안으로 활용될 수 있다. 그리고 위험관리를 시스템 구축이나 규정의 개선이 아닌 응용프로그램 관점으로 방안을 제시했다는 점에서 관련한 연구의 기초가 될 수 있을 것으로 생각한다.

### 5.2 한계 및 향후 발전방향

본 논문에서는 은행 시스템에서 사용되고 있는 IT공통모듈을 사례로 자료를 수집함으로써 타금융권을 포함한 자료의 수집에 한계가 있었다. 그리고 리스크의 크기를 거래금액만 반영하여 분석한 한계점을 지니고 있다.

향후 연구에서는 금융IT를 포함한 다양한 산업 군에서의 관련 자료를 바탕으로 한 추가 연구가 이루어진다면, 보다 일반적인 기준으로 사용될 수 것으로 기대한다.

## References


[1] Financial Supervisory Service, "Integrated risk management best practices under Basel II(Vol.2 operations/interest rate/liquidity risk," internal capital adequacy), Dec. 2008

[2] Young-jae Lee, Introduction to BCP, Digital times Publishers, Feb. 2004

[3] Se-kyung Oh, Risk Management Theory, Kyungmoon Publishers, Feb. 1999.

[4] The Bank of Korea, "Recent Domestic Bank's Risk Management and Future Works," Finance Systems Review,Vol.7, pp.85-95, 2002

[5] Jong-ho Kim, "The importance of operational risk and measurement," Daeeun Economic Review, 172, pp.42-49, Mar. 2001

[6] Young-chan Yang, "A Study on Audit Framework of IT Operation Risk for Compliance with Basel Ⅱ," The Graduate School of Konkuk University, Aug. 2009

[7] Kyung-jin Lim, "A study on the risk managements of financial institutions," Graduate school of Chonbuk National University, Aug. 2002

[8] Liu Tong, "A study on commercial banks′ operational risk management in China," Graduate school of Sungkyunkwan

University, Nov. 2011
〔9〕 Il-yong Ko, "Basel Ⅱ operational risk - the new challenge," Risk review, No. 7, Financial Supervisory Service, Feb. 2006
〔10〕 Jeong-ryul Kim, "A discussion of the operational risk management for financial institutions," Korea deposit insurance coporation, KDIC Financial Research 5(1), pp.131-165, Mar. 2004
〔11〕 Seok-ho Sunwoo and Eun-young Jun, "Quantifying operational risk and testing fitness of loss distribution," Korea Institute of finance, Dec. 2006
〔12〕 Seung-kook Lee, "Characteristics of domestic banks' operational risk analysis: Analysis of internal loss data," Risk review, pp.173-191, Financial Supervisory Service, Sep. 2006
〔13〕 Hiwatahi, Junji and Hiroshi Ashida, "Advancing Operational Risk Ma-nagement Using Japanese Banking Experience," Federal Reserve Bank of Chicago, Dec. 2002.
〔14〕 Young-Jai Lee and Myung-Soo Hwang, "The Mitigation Model Development for Minimizing IT Operational Risks," Dongkuk University, Sep. 2007
〔15〕 Young-gon Kim, "A study on the operational risk management of financial institution," Konkuk University, Dec. 2002
〔16〕 Hyang-su Park, "Recent domestic banks' risk management status and future challenges," The Bank of Korea Financial System Review, no. 7, pp.85-95, Aug. 2002
〔17〕 Tae-Hong Kang and Sung-Yul Rhew, "A Study on Extraction of Defect Causal Variables for Defect Management in Financial Information System," Soongsil University, Feb. 2013
〔18〕 "Electronic banking supervision regulations," Financial Services Commission Notice No. 2013-44, Dec. 2013
〔19〕 Yong-sub Kim, "A study on construction of the disaster recovery systems in the financial institutions," Graduate school of Software Sejong University, Dec. 2002
〔20〕 Hyun-ju Shin, "The risk management system and new improvement," Business administration of Dongguk University, Dec. 1999
〔21〕 Young-joun Youn, "An empirical study on risk factors of the IT projects implemented by financial institutions," Graduate school of Engineering Yonsei University, Dec. 2005
〔22〕 Seung-mi Hong, "A study on Risk Management of Banks in Korea," Graduate School of Economics Yonsei University, Dec. 2002
〔23〕 Dong-jin Park, "A study on the management program for operational risk of financial institutions," Graduate school of Sungkyunkwan University, Dec. 2010
〔24〕 Korea Institute of Finance, "Advanced operational risk management practices of financial institutions and future challenges," Weekly International Financial Trends, 9(34), pp.20-26, 2000

## 〈저자소개〉

조 성 철 (Seong-Cheol Cho) 정회원
2000년 2월: 인하대학교 전자계산공학과 학사
2000년 1월~현재: KB국민은행 전산정보본부
2013년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 금융정보보안, 위험관리

남 초 이 (Cho-Yee Nam) 학생회원
2013년 2월: 서울여자대학교 정보보호학과 학사
2014년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 금융정보보안, 위험관리

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, nhn, 시큐베이스 등 근무
2011년 9월~현재: 고려대학교 정보보호대학원 조교수
〈관심분야〉 위험관리, 정보보호컨설팅, 정보보호 및 개인정보보호정책