Journal of the Korea Academia-Industrial cooperation Society
Vol. 15, No. 1 pp. 460-465, 2014

http://dx.doi.org/10.5762/KAIS.2014.15.1.460

컴플라이언스 매니지먼트 서비스를 위한 기술적 접근에 관한 연구

이준호[1*], 오해석[2]
[1](주)코스콤 인프라사업부, [2]가천대학교 IT대학

A Study on Technical Approach for Compliance Management Service

Jun-Ho Lee[1*] and Hea-seok Oh[2]
[1]**Division of IT Infra Business, Koscom Corporation**
[2]**Division of IT, Gachon University**

요 약 전자금융 시대를 살고 있는 지금 안전한 전자금융거래를 위해 금융감독기관의 규제가 지속적으로 강화되고 있다. 하지만 규제를 준수해야 하는 약 4,500여개 금융기관의 수에 비해 정보보호컨설팅 및 정보보호서비스 사업자의 수가 턱없이 부족하고 감독기관의 물리적 감독업무에도 상당한 업무부담이 과중되고 있다. 날로 실시간 리스크관리의 요구가 강해지고 있는바 본 논문을 통하여 규제준수에 관해 요건, 이행, 모니터링, 감독 등의 업무를 효율적으로 하기 위해 필요한 기술적 접근을 시도하고 시스템 기반의 컴플라이언스 매니지먼트를 위한 요소항목을 도출하고자 한다. 본 연구는 금융IT 컴플라이언스 매니지먼트 프레임워크와 GRC 프로세스 모델을 기반으로 연구하였고 연구결과 컴플라이언스 매니지먼트 라이프사이클과 각 라이프사이클에 따른 34개의 컴플라이언스 매니지먼트 인덱스를 설계하였다.

Abstract The Financial Supervisory Institution constantly has tightened the regulation for secure electronic financial service. Information Security Consulting and Service companies are not enough to cover about 4,500 financial institutes required to comply with the regulation, and the Financial Supervisory Institution also suffers from work overload. The demand for real-time work of risk management is getting stronger. Compliance with the regulation has to be attempted with technical approach so that requirement, implementation, monitoring, and supervision are efficiently performed. And, articles have to be concluded with compliance management service. In this research used compliance management framework and IT GRC process model, have to be designed compliance management lifecycle and 34 index.

Key Words : Compliance Management, GRC, Risk Management

1. 서론

인터넷뱅킹 계좌 등록수가 8,000만명이 넘을 정도로 전자금융거래가 활발해진만큼 금융정보탈취를 목적으로 하는 해킹 또한 지속적으로 증가하였고 안전한 전자금융거래를 위해 금융감독기관은 금융기관이 준수해야 하는 다양한 규제를 발표하였다[12,13]. 금융기관이 전자금융거래시 반드시 준수해야 하는 법령은 전자금융거래법이다. 금융위원회는 전자금융거래법 시행령, 시행규칙과 함께 전자금융거래 준수여부를 감독하기 위한 전자금융감독규정을 제정한바 있다. 또한 금융위원회는 전자금융거래의 안전성을 확보하기 위해 “금융회사 정보기술(IT)부문 보호업무 모범규준(이하 “모범규준”)을 제정하였고 사실상의 모든 금융기관은 전자금융거래법 시행령·시행규

*Corresponding Author : Jun-Ho Lee(Koscom Corporation)
Tel: +82-10-3765-8793 email: jhlee@koscom.co.kr
Received November 28, 2013 Revised January 8, 2014 Accepted January 9, 2014

칙, 전자금융감독규정 및 모범규준 등 금융위에서 주관하는 각종 컴플라이언스(이하 '금융IT 컴플라이언스'라 한다)를 준수해야 한다[7-11]. 문제는 금융IT 컴플라이언스를 준수해야 하는 금융기관 수가 4,500여 기관에 달한다는 것이다. 금융 IT 컴플라이언스'를 준수해야 하는 금융기관의 수가 많은 것만이 문제가 아니다. 금융IT 컴플라이언스를 준수하기 위하여 금융기관은 예산의 배정과 함께 조직의 구성, 솔루션의 도입 및 정보보호 컨설팅을 주기적으로 받고 취약점 분석 결과를 금융감독기관에 보고하여야 한다. 하지만 취약점 분석▪평가를 자체적으로 수행할 수 있는 금융기관은 극히 제한적이기 때문에 법에 의해 취약점 분석▪평가를 할 수 있는 자격을 가진 정보보호컨설팅전문업체 또는 정보공유분석센터를 통해 그 결과를 득해야 한다. 문제는 정보보호컨설팅을 수행할 수 있는 자격을 가진 기관의 수가 10개 미만으로 대상금융기관의 수에 비해 턱없이 부족하다는 점이다. 이에 따라 금융감독기관 또한 모든 금융기관을 대상으로 한 실태조사 등 감독업무를 수행하기에 어려움이 따른다. 따라서 금융IT 컴플라이언스를 준수해야하는 금융기관, 감독기관 및 금융IT컴플라이언스를 지원하는 정보보호사업자 모두 시스템기반의 금융IT 컴플라이언스 매니지먼트가 필요하다.

본 논문에서는 시스템기반의 금융IT 컴플라이언스 매니지먼트 서비스를 위하여 고려해야 하는 기술적 요소에 대한 분석하고 컴플라이언스 매니지먼트 서비스를 위한 프로세스를 제안하고자 한다. 본 논문의 구성은 다음과 같다. 2장에서는 관련 연구 내용을 분석하고 3장에서는 컴플라이언스 매니지먼트 서비스를 위한 기술적 요소를 분석하고 서비스 프로세스를 제안한다. 끝으로 결론 및 향후 연구방향을 제시한다.

2. 본론

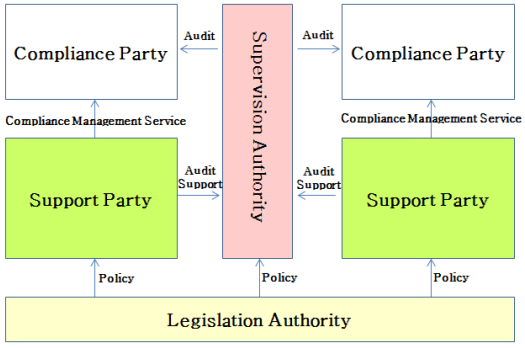
본 장에서는 선행 연구된 금융IT보안 컴플라이언스 매니지먼트 프레임워크를 분석하고 컴플라이언스 매니지먼트 프로세스가 궁극적으로 지향하는 IT GRC 프로세스 모델에 대해 분석하고자 한다.

2.1 금융IT 컴플라이언스 매니지먼트 프레임워크

본 연구에 앞서 선행 연구된 금융IT 컴플라이언스 매니지먼트 프레임워크에서 금융IT 컴플라이언스 매니지먼트 서비스에 참여자를 제정기관, 감독기관, 준수기관, 지원기관으로 정의하였고 각 참여기관 간 상호 연관성 및 역할을 정의하였다.[8]

[Table 1] Role of Compliance Management Service Participants

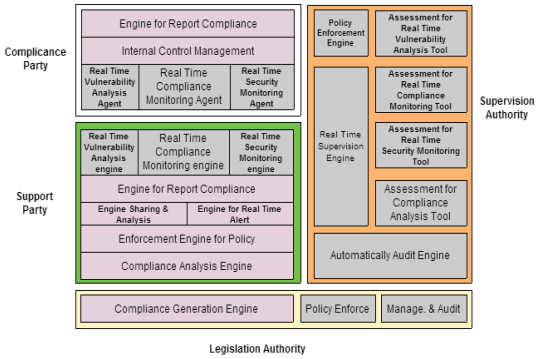
Participant	Definition
Legislation Authority	Authority to enact law and standard ex) Congress, FSC, MOSPA etc.
Supervision Authority	Authority to supervise implementation of compliance ex) FSS, Division Audit etc.
Compliance Party	Party that comply with the law ex) Financial Institute, Company
Support Party	Support Party that comply with the law and standards etc. ex) Financial ISAC, security agency



[Fig. 1] Participants Structure

각 참여기관 간 역할구조는 Fig. 1와 같다. 제정기관은 컴플라이언스를 제정하고 감독기관을 관리 감독한다. 제정기관은 지원기관과 상호 협력하는 구조를 가지며 지원기관은 감독기관을 보좌한다. 컴플라이언스 준수기관은 감독기관의 감독을 받으면서 지원기관으로부터 컴플라이언스 매니지먼트 서비스를 받는다.

또한 각 참여기관에서 보유하여야 하는 기능적 정의를 Fig. 2와 같이 하였다. 그러나 참여기관별로 기능적 정의는 이루었으나 각 항목에 대해 상세한 기술적 요소는 추후 연구과제로 남겨진 바 있다. 이러한 기술적 접근을 이루기 위한 요소 항목을 설계하고 컴플라이언스 매니지먼트 서비스를 위한 프로세스를 본 논문에서 제안하고자 한다.

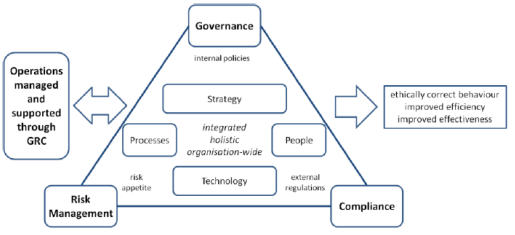


[Fig. 2] Functions of Participants

2.2 IT GRC 프로세스 모델 분석

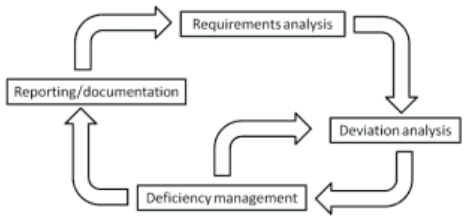
GRC(Governance, Risk and Compliance)라는 용어는 최근 몇 년간 비즈니스 이슈로 크게 부각이 되었다. GRC라는 용어는 PWC가 2004년 최초로 사용하기 시작했는데 PWC는 GRC자체가 새로운 것이 아니고 개별적인 이슈로써 거버넌스, 리스크 관리 그리고 규제준수라는 것은 기업의 근본적인 걱정거리로 항상 있어왔다고 표현하고 있다[3].

PWC가 GRC를 처음 정의하면서 여러 가지 연구가 있었지만 IT GRC에 대해서 과학적인 접근의 연구를 이룬 것은 니콜라스 라쓰에 의해서이다[2]. 니콜라스 라쓰는 우선 통합 GRC 연구를 위한 참조 프레임을 설계하였다 [Fig. 3].



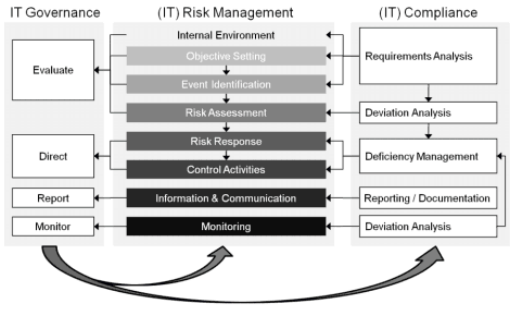
[Fig. 3] Elements in focus in the frame of reference for GRC research

이후 니콜라스 라쓰는 IT 거버넌스, 위험 관리, IT 컴플라이언스 통합을 위한 프로세스 모델을 수립하였다. 즉 IT GRC에 관한 프로세스 모델을 정립한 것이다[1]. 라쓰는 IT 컴플라이언스 프로세스 모델을 요구조건 분석, 이탈 분석, 결함 관리, 문서화/보고의 4가지 프로세스로 정의하였다.



[Fig. 4] IT Compliance Process Model

또한 ISO/IEC 38500:2008 모델에서 정의한 IT 거버넌스 프로세스와 COSO ERM에서 정의한 Risk Management 프로세스를 통합하여 IT GRC 관리를 위한 프로세스 모델을 정의하였다[1,5,6].



[Fig. 5] Integrated IT GRC Process Model

대한민국 또한 각종 규제가 강화되고 리스크 관리 이슈가 증가하면서 IT GRC에 대한 니즈는 증가하였지만 IT GRC를 위한 학술적 연구는 이제 시작이다. 본 논문에서는 사전 연구된 금융IT 컴플라이언스 프레임워크와 통합 IT GRC 프로세스 모델 중 컴플라이언스 매니지먼트 서비스를 하기 위한 기술적 요소 항목을 설계하고자 한다.

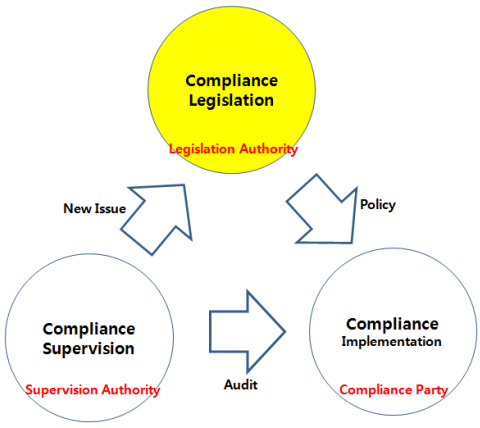
2.3 컴플라이언스 매니지먼트 서비스를 위한 기술적 접근

본 장에서는 인력기반으로 컴플라이언스를 준수여부를 확인할 수 밖에 없는 현실에 보다 효율적이고 즉시성이 반영된 컴플라이언스 준수 여부를 확인할 수 있는 기술적 접근을 시도하고자 한다. 본 장에서 사용하는 용어는 사전 연구된 금융IT 컴플라이언스 매니지먼트 프레임워크에서 정의한 참여기관의 용어를 사용하고자 하며 참여기관 별 상세기능에서 정의한 항목의 구체적인 기술적 요소항목을 도출하고 시스템화가 가능한 프로세스를 설계하고자 한다.

2.3.1 컴플라이언스 매니지먼트 인덱스 설계

컴플라이언스 매니지먼트 서비스를 위한 기술적 접근을 위해 먼저 인덱스의 설계가 필요하다. 컴플라이언스 매니지먼트는 기술적 이슈보다는 관리적 이슈가 강하기 때문에 이를 시스템으로 구현하기 위해서는 관리적 이슈를 프로세스 기반으로 통제하기 위한 분류와 인덱스에 대한 설계가 필요하다.

우선 컴플라이언스 라이프사이클은 기본적으로 제정기관이 컴플라이언스를 제정하고 준수기관은 이를 준수한다. 그리고 감독기관은 주기적으로 준수기관의 규제준수여부를 감독하며 새로운 이슈를 제정기관에 보고함으로써 컴플라이언스의 개정이 일어나는 기본적 구조를 가지고 있다[Fig. 6].



[Fig. 6] Compliance Lifecycle

컴플라이언스 매니지먼트서비스가 기술적으로 구현되기 위해서는 컴플라이언스 라이프사이클을 모두 반영해야만 한다. 따라서 컴플라이언스 매니지먼트 인덱스를 컴플라이언스 라이프사이클을 기준으로 설계하고자 한다[Table 2].

컴플라이언스 매니지먼트를 위한 인덱스 설계는 우선 각 참여기관의 역할을 기준으로 하였다. 제정기관의 경우 컴플라이언스를 제·개정 하는 것이 전부이기 때문에 인덱스 설계가 간단하다. 컴플라이언스를 제정하는 제정기관 코드(L), 관련 컴플라이언스명(LN), 제정년도(YYYY), 그리고 컴플라이언스 조·항·호를 정의하는 번호(N_N_N)이다. 다만 컴플라이언스의 각 조항이 관리적 측면(M)에 해당하는 것인지 기술적 측면(N)에 해당하는 것이지 분류코드를 둘 수 있다. 이와 관련하여 컴플라이언스를 제정하는 제정기관이 다양하고 각 제정기관별로 다양한 종류의 컴플라이언스가 존재할 수 있다. 또한 내부통제까지 감안하였을 때 컴플라이언스 제정기관 관련 분류표는 매우 다양해질 수 있다. 다만, 이에 대해서는 표준화가 필요하며 이는 본 논문의 주제를 벗어나므로 본 논문에서는 다루지 않는 것으로 한다.

[Table 2] Compliance Management Index

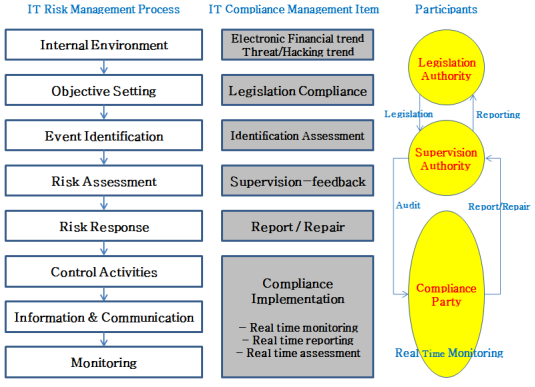
Item	Code	Compliance Management Index
Compliance Legislation	L	- L : Legislation Institute Code - LN : Compliance Name - YYYY : Legislation Date - N_N_N : Article of Law - M : Management article - T : Technical article
Compliance Supervision	A	- A : Audit Institute Code - LN : Compliance Name - M/T : Mgmt./Tech. article - An : Audit No. (n=000~999) - N_N_N : Article of Law - C : Compliance Institure Code - AP : Pass of Audit - APn : Accumulation of AP - ANP : Non-Pass of Audit - ANPn : Accumulation of ANP - AS : Audit Suspension - ASn : Accumulation of AS - YYYYMMDD : Audit Date
Compliance Implementation	C	- L : Legislation Institute Code - LN : Compliance Name - YYYY : Legislation Date - A : Audit Institute Code - C : Compliance Institure Code - M/T : Mgmt./Tech. article - An : Audit No. (n=000~999) - N_N_N : Article of Law - AP : Pass of Audit - APn : Accumulation of AP - ANP : Non-Pass of Audit - ANPn : Accumulation of ANP - AS : Audit Suspension - ASn : Accumulation of AS - YYYYMMDD : Audit Date

다음으로 컴플라이언스 감독기관의 인덱스는 실제 감독업무에 필요한 코드가 추가되게 된다. 쉽게 표현하여 감독기관이 어떤 컴플라이언스에 대해 준수기관이 제대로 준수하는지를 감독하는 것이기 때문에 관련 인덱스를 정의하였고, 추적관리를 위하여 검사 통과/미통과/보류와 관련한 인덱스를 별도로 설계하였다. 다음으로 컴플라이언스 준수기관의 경우 어떠한 컴플라이언스를 잘 준수하고 있는 지의 여부를 판단할 수 있도록 인덱스를 설계하였다.

2.3.2 컴플라이언스 매니지먼트 프로세스 설계

본 절에서는 컴플라이언스 매니지먼트 서비스가 기술적으로 구현되기 위한 프로세스를 설계하고자 한다. 본 프로세스는 COSO에서 정의한 Risk Management Framework[6]의 프로세스를 바탕으로 하였으며 제정기관, 감독기관, 준수기관 등 참여기관의 역할과 요구사항에 맞게끔 반영을 하여 설계하였다[Fig. 7].

컴플라이언스 매니지먼트는 결국 리스크관리의 큰 틀에서 이해할 수 있다. 또한 본 논문에서 설계한 각 참여기관의 역할에 따라 IT 컴플라이언스 매니지먼트에 필요한 항목을 각 참여기관별로 Fig. 7과 같이 대응할 수 있으며 3.1절에서 설계한 인덱스를 바탕으로 컴플라이언스 매지니먼트 서비스에 필요한 각 서비스 항목별로 구체적인 프로세스를 설계할 수 있다. 각 서비스항목별 상세 프로세스 설계는 본 논문의 범위를 벗어나므로 추후 연구과제로 남기고자 한다.



[Fig. 7] Compliance Management Process

3. 결론

현재의 전자금융 환경에서 주어진 금융IT 컴플라이언스는 감독기관과 준수기관 모두에게 부담되고 효율성이 부족하다. 본 논문에서는 보다 효율적인 컴플라이언스 매니지먼트 서비스를 위한 기술적 요소항목에 대한 접근을 하였고 기술적 접근에 필요한 인덱스의 설계와 서비스 프로세스의 기본 틀을 설계하였다. 컴플라이언스 매니지먼트 서비스는 반드시 실시간성과 효율성이 반영되어야 하는 만큼 본 연구는 반드시 필요하고 추후 연구 과제로 남겨진 상세 서비스 항목별 프로세스 설계를 본 연구에 이어 수행해보고자 한다. IT Complianc Managment, IT Risk Management IT Governance는 상호 연관성이 있으며 이미 GRC라는 분야로 연구가 활발히 진행되고 있는 바 본 연구를 확대하여 IT GRC 매니지먼트 서비스를 위한 기술적 분석에 대한 연구로 향후 확대하고자 한다.

References

[1] N. Racz, E. Weippl, and A. Seufert, "A process model for integrated IT governance, risk, and compliance management," Databases and Information Systems, Proc. of the Ninth Internantional Baltic Conference(DB &IS 2010), Riga University Press, Jul. 2010. pp. 155-170.

[2] Racz, N., Weippl, E. & Seufert, A.: A frame of reference for research of integrated governance, risk, and compliance (GRC). In: Proceedings of the 11th TC11 Conference on Communications and Multimedia Security (2010)

[3] PricewaterhouseCoopers: Integrity-Driven Performance. A New Strategy for Success Through Integrated Governance, Risk and Compliance Management. http://www.globalcompliance.com/pdf/PwCIntegrityDrivenPerformance.pdf (2004)

[4] Frigo, M.L., Anderson, R.J.: A Strategic Framework for Governance, Risk, and Compliance. Strategic Finance 44:1, 20-61(2009)

[5] ISO/IEC 38500:2008. Corporate governance of information technology, ISO/IEC

[6] COSO: Enterprise risk management framework. www.coso.org(2004)

[7] Taehee Kim, YoungTae Kim, Jaemo Sung “Study on Financial IT Security Compliance Framework” 35th Korea Information Processing Society Spring Conference 18 1, 2011

[8] Junho Lee, Haeseok Oh, “The Research for Financial IT Compliance Management Framework based on Cloud" Korea Society of IT Services Spring Conrerence Paper, 2013

[9] Financial Security Agency, “Report of IT Compliance Analysis on Financial Sector” 2009

[10] Financial Security Agency, “Financial IT Security Compliance Research”, TTAK.KO-12.0179, TTA, 2011

[11] Telecommunication Technology Association, “Financial Information Security Compliance Framework”, 2011

[12] Financial Services Commission "Standard for Information Technology Security in Financial Institutes”, 2011

[13] Bank of Korea “Internet Banking Statistics 2012 in Korea”, 2013

이 준 호(Jun-Ho Lee) **[정회원]**

- 1994년 2월 : 광운대학교 수학과 (학사)
- 1997년 2월 : 광운대학교 수학과 (이학석사)
- 1996년 3월 ~ 1999년 3월 : 백두정보기술연구소 선임연구원
- 1999년 6월 ~ 현재 : ㈜코스콤 인프라본부 근무

<관심분야>
정보보호, 정보통신, 경영정보

오 해 석(Hea-Seok Oh) **[정회원]**

- 1975년 2월 : 서울대학교 계산통계학과(학사)
- 1981년 2월 : 서울대학교 계산통계학과(공학석사)
- 1989년 2월 : 서울대학교 계산통계학과(공학박사)
- 1982년 1월 ~ 2003년 2월 : 숭실대학교 컴퓨터학부 교수/부총장(역임)
- 2003년 3월 ~ 현재 : 가천대학교 IT대학 교수
- 2009년 9월 ~ 현재 : 대통령 IT 특별보좌관

<관심분야>
멀티미디어, 데이터베이스, 지식경영, 정보통신