Journal of The Korea Institute of Information Security & Cryptology ISSN 1598-3986(Print)
VOL.31, NO.4, Aug. 2021 ISSN 2288-2715(Online)
https://doi.org/10.13089/JKIISC.2021.31.4.763

공공부문 정보보안 SLA 성과체계 사례연구

정 재 호,[1†] 김 휘 강[2‡]
[1,2]고려대학교 (대학원생, 교수)

Case Study Plan for Information Security SLA Performance System in Public Sector

Jae Ho Jeong,[1†] Huy Kang Kim[2‡]
[1,2]Korea University (Graduate student, Professor)

요 약

정보보안은 IT 운영프로세스로 시작하여 지금은 정보기술의 중요한 문제로 인식되면서 각 국제단체에서 개념을 새롭게 규정하고 있다. 정보보안 자체가 IT기술들의 새로운 조합으로 하나의 기술 집합이고 기술영역이다. 많은 공공부문에서 IT 아웃소싱이 일반화되면서 SLA(Service Level Agreement)를 도입하여 IT서비스 수준에 대해 평가를 한다. 정보보안 영역에서 SLA 성과지표 도출과 선정에 대한 많은 연구는 진행되었지만, 성과지표의 서비스 수준 평가, 성과체계에 대한 적용방안은 찾기 어렵다.

이 논문은 공공부문을 기반으로 하는 정보보안 성과지표의 서비스 평가 체계와 보상 규정이 포함된 성과체계 적용에 대한 연구를 수행하였다. 특정 공공부문의 환경과 특성을 고려한 성과지표의 기대치와 목표치를 정의하는 기준과 보상(인센티브・페널티) 규정을 제시하고 적절한 SLA 비용을 정의한다.

ABSTRACT

Information security started as an IT operation process and is now recognized as an important issue of information technology, and each international organization is newly defining the concept. Information security itself is a new combination of IT technologies, a set of technologies and a technology area. As IT outsourcing becomes common in many public sectors, SLAs are introduced to evaluate the level of IT services. In the area of information security, many studies have been conducted on the derivation and selection of SLA performance indicators, but it is difficult to find a way to apply the performance indicators to service level evaluation and performance systems.

This thesis conducted a study on the application of a service evaluation system for information security performance indicators based on the public sector and a performance system including compensation regulations. It presents standards and rewards(incentive and penalty) that define expectation and targets of performance indicators that take into account the environment and characteristics of a specific public sector, and defines appropriate SLA costs. It proposes a change plan for the organizational structure for practical SLA application and service level improvement.

Keywords: SLA Measurement, Evaluation, Incentive and Penalty

I. 서 론

IT 발전은 비즈니스를 지원하는 인프라에 국한되지 않고 경영 전반의 프로세스를 지원하는 새로운 기회로 인식되면서 많은 변화를 가져오고 있다. 이러한 패러다임의 변화 속에서 내·외부의 불법적 침입으

Received(04. 13. 2021), Modified(05. 31. 2021), Accepted(06. 21. 2021)

† 주저자, bboyaa69@korea.ac.kr
‡ 교신저자, cenda@korea.ac.kr(Corresponding author)

로부터 정보자원을 보호하는 정보보안은 기밀성, 무결성, 가용성을 높여서 기업의 경쟁력 확보를 목표로 한다. 정보화촉진 기본법 2조 4항에 정보의 수집·가공·저장·검색·송신·수신 중에 정보의 훼손, 변조, 유출 등을 방지하기 위한 관리적·기술적 수단을 마련하는 것으로 명시되어 있으며, 이는 비즈니스 프로세스를 지원하는 IT 인프라에서 제품이나 서비스를 제공하는 과정까지 조직, 자원, 인력, 정보 등에 대한 전반적인 시스템을 보호하는 용어로 사용되고 있다.

정보보안 관리체계는 관리적 보안, 기술적 보안, 물리적 보안의 세 가지 영역으로 나눌 수 있고 정보보안 SLA 적용은 기술적 보안을 기반으로 구축되고 이행되는 관리적 보안의 영역이다.

공공부문 IT는 IT 전문기업의 아웃소싱을 통해 운영되고 있다. 보안은 어떤 내재하는 취약성에 의해 제기되는 다양한 위협으로부터 자산을 보호하는 것이다. 보안 프로세스는 일반적으로 이러한 취약성에 의해 제기된 위험을 감소시키는 것을 돕는 보안 통제의 선택과 구현을 다룬다.[7] 정보보안에서 IT 인프라는 취약성의 근본적인 원인이고 보호를 받아야 하는 자산이다. 이런 관계에 의해 정보보안은 IT아웃소싱의 일부분으로 계약되고 운영되어 진다. 정보보안에 대한 내·외부위협을 IT 생명주기로 본다면 수요자 요구사항에 맞는 하드웨어와 소프트웨어를 설계 후 구축하고 배포, 구축, 배치, 운영 및 유지보수, 폐기 등의 과정에서 다양한 공격이 증가하고 있다.

정보보안에 대한 공격은 기업의 비즈니스에 큰 악영향으로 막대한 손실을 가져오며 영구히 복구할 수 없는 심각한 상황을 초래할 수 있다. 이런 상황을 방지하기 위해 기업은 아웃소싱업체의 서비스 수준 향상을 고민하며 지속적인 고도화를 요구한다.

기업에서는 IT아웃소싱 업체의 서비스 제공 수준을 보장받고 지속적인 개선을 위해 SLA (Service Level Agreement) 추진을 수행한다. SLA 추진은 전면적인 IT아웃소싱에서 진행되었고 많은 영역에서 성과를 이루었다. SLA 계약은 전반적이고 일반적인 IT 운영영역을 다루고 있다.

그러나, 현 추세에서는 정보보안 관리는 IT 관리와 개념적으로 구분되는 추세이고, 정보보안은 IT 자산을 대상으로 취약점을 제거하고 정부 지침이나 가이드라인을 준수하여 위험을 최소화하는 업무이다. 가장 민감한 분야인 관계로 좀 더 명확하고 세부적인 계약을 요구하게 된다. 정보보안은 이전과 달리 IT 운영 수준이 높다고 보안 위협에 안전하다고 생각 할 수 있는 것은 아니다.

따라서, 정보보안을 위해 어떤 활동을 수행해야 하는지를 확인하고 수행해야 하는 활동을 명시해야 하고 정보보안 SLA 계약에 포함되어야 한다. 본 논문에서는 정보보안의 근본이 되는 정보 인프라와 네트워크 인프라의 신속한 보안 통제 및 업무 처리를 위한 IT 운영프로세스를 분석함과 동시에 정보보안의 취약점 제거 및 자산 보호를 위한 체크리스트의 정기적인 확인을 위한 업무를 성과지표로 도출한다. 정보보안 강화를 위한 IT 이해관계자들이 수행해야 할 성과지표를 선정한다.

정보보안의 체크리스트와 IT 운영 프로세스 분석을 통해 정보보안 SLA 성과지표 Pool을 생성하고 설문조사를 통한 성과지표 선정과 동시에 정보보안 서비스 수준 향상을 위한 적용 방안을 제시한다.

- Day to Day로 발생하는 운영프로세스 성과지표를 확인하고 서비스 수준 향상을 위한 성과지표를 도출해야 한다.
- 타 연구에서 정의된 정보보안 성과지표를 비교하여 최적화된 성과지표를 선정한다.
- 정보보안 성과지표와 운영프로세스 강화를 위한 성과지표들의 중요도에 따른 서비스 제공 능력을 평가하는 방안을 마련한다.
- 아웃소싱업체 서비스 제공 수준에 따른 정보보안 SLA 보상체계를 정립하여 적용 할 수 있는 방안을 제시한다.

위와 같은 정보보안 관련 과제에 대한 해답을 도출하기 위해 성과지표 비율에 따른 SLA 측정 기준 적용 및 보상방안을 중점적으로 연구한다.

II. 관련 연구

2.1 IT아웃소싱과 정보보안

과거 기업은 비즈니스 영역에서 경쟁력 우위 확보를 위해 모든 유관분야의 역량을 내재화하거나 인수·합병을 통해 기술을 소유하였지만, 현재는 기업의 핵심 역량에 집중하고 비주력분야는 전문업체를 통해 경영 환경 변화에 따른 양질의 서비스를 받음과 동시에 최소 비용을 통한 효율적 운영과 관리를 추구하는 것이 일반적이다.

기업 목표달성을 위해 IT 개발 및 운영기능의 일

부분 혹은 전부를 외부 전문업체에 위탁하여 수행하는 활동을 IT 아웃소싱이라 하고, 이를 위해서는 고객사와 공급 사간 일련의 계약과 계약관리의 행위가 필요하다. IT 아웃소싱은 추진 방식과 서비스 형태 및 자산 소유 형태에 따라 다양한 유형이 존재하며, 조직의 관리 주체와 특성에 따라 다양한 방식의 계약을 진행한다. 아웃소싱 계약은 초기에 토탈 아웃소싱 방식이 지배적이었으나, 운영 환경의 변화와 IT분야별 가치 변화에 따라 선택적 아웃소싱방식으로 전환되고 있다.

IT가 인터넷 시대를 맞이하면서 IT의 일부분이었던 정보보안은 중요성이 확대되어 갔다. 이에 정부와 행정기관은 정보보안 부문의 지침과 연구보고서를 별도로 제시하면서 IT 운영과 정보보안은 개념적으로 분리되는 양상을 보였다. 현재도 IT 운영의 일부분으로 정보보안 관리가 포함되었기에 보안시스템 관련 운영 프로세스는 지금도 공유하고 있다.

그러나, 정보보안의 중요성이 확대됨에 따라 각 기업에서는 IT 관리부서와 별도로 보안 관리 부서를 독립시키고 있으며, 보안 관리 부서는 물리적 보안뿐만 아니라 정보보안 분야 관리체계 수립 및 이행을 독자적으로 수행하고 있다. IT 관리 분야와 정보보안 분야는 상호 발생하는 요구사항을 충족시키기 위해 상호 간 협업과 감시를 통해 관리를 수행한다. 이에 아웃소싱 수준 향상을 위한 SLA는 정보보안에 특화된 계약 체결이 요구되어 진다. 정부 기관의 지침과 가이드라인에서 의무적 이행 규정이 생기면서 정보보안 SLA 성과지표의 선정이 필요해졌다.

관리체계의 분화는 관리체계 요구사항에 맞는 SLA 필요성이 대두되었고 많은 기업에서 수행되고 있는 SLA는 IT 부문과 정보보안 부문으로 분화되는 양상을 보이고고 있다. 이 논문에서는 이러한 현상에 따라 보안 SLA 성과지표를 선정·측정하고 중요도에 따른 비율에 따라 보상체계를 적용하는 방안을 제시하려고 한다.

2.2 ITSM(IT Service Management)과 ITIL(IT Infrastructure Library)[8][9][10]

공공부문 IT서비스는 외부 전문업체를 통해 IT유지보수를 관리하는 아웃소싱 형태가 주류를 이루고 있으며 IT인프라나 플랫폼까지도 외부 전문업체에 위탁하고 있다. 이런 변화에 따라 서비스 이용업체는 외부에서 제공하는 서비스가 만족할 만한 수준의 서비스를 제공 받고 있는 지를 판단해야 한다.

IT아웃소싱을 수행하면서 서비스 품질에 대한 많은 문제점이 발생하였다. 담당자간 의사소통 부족으로 인한 장애발생, 비즈니스 요구사항에 맞지 않는 IT운영, 시스템 운영 및 프로세스의 개선 없는 정체 등이다. 이에 IT서비스를 관리하기 위한 프로세스 도입이 진행되었다. ITSM 영역에서의 대표적인 프로세스 모델은 eSCM, CMMI, ITIL 그리고 COBIT 등이 있다.[8][9] <Table 1>은 각 프로세스 모델별 특징을 나타낸다.

Table 1. ITSM Process Model

Process Model	Definition	Scope	Specification
e-SCM (e-Sourcing Capability Model)	▪ The e-sourcing competency evaluation model first released version 1.0 in November 2001 by the IT Services Qualification Center (ITSQC) of Carnegie Mellon University in the United States. ▪ To objectively evaluate the competency level of service providers and improve the quality level in IT outsourcing	▪ IT Outsourcing Business Life Cycle	▪ Model for IT outsourcing business selection and management ▪ 5-step competency certification model
ITIL	▪ Best practice library in ITSM ▪ Initially, mainly IT infrastructure operation ▪ Divided into all process areas required for monitoring and areas to operate and support them	▪ the Service Lifecycle from IT planning to service design, operation, improvement, and strategy	▪ Process optimization through best practices ▪ Continuous improvement through plan-do-check-act activities
CMMI (Capability Maturity Model Integration)	▪ Best Practices in System Design/Build ▪ Certification model for systems engineering maturity	▪ Systems analysis, design, development and testing process	▪ 4 areas including process management, project management, engineering, and support ▪ Define organizational maturity from Level 1 (Initial) to Level 5 (Optimizing)
COBIT (Control Objective for Information and Technology)	▪ IT management model developed by ISACA (Information System Audit and Control Association) ▪ To achieve control objectives for IT and provide guidance on IT governance	▪ Planning, organization, introduction and construction, operation/support, monitoring area throughout the IT management process	▪ Used in guidelines for comprehensive management systems for managers and IT managers ▪ Use of IT audit tools

ITSM의 기반이 되는 프레임워크를 제공하는 프로세스 모델에서 주로 활용된 ITIL기반의 운영 프로세스는 많은 문제점을 해결하거나 최소화했다. 고객의 요구(Needs)를 이해하고 지속해서 높은 품질의 서비스를 제공하기 위해 프로세스 운영 및 지속적인 개선을 통해 경쟁우위를 확보하는 것이다. ITIL기반의 운영프로세스는 Plan-Do-Check-Act 활동을 통해 지속적인 개선을 목표로 기업의 환경에 따라 적합한 운영 프로세스를 도입하여 운영하였다. ITIL은 기업 내의 복잡한 IT 환경에 대해 비즈니스를 지원하는 서비스 중심의 최적의 프레임워크를 제시하며, 모든 조직이나 기업에도 활용할 수 있고 어떤 벤더에도 종속되지 않는 포괄적이고 공개적인 표준가이드이다.[8][9] 또한, 국내에서 ITSM구축이나 IT 운영 프로세스 구현 시 가장 보편적으로 사용되는 프레임워크이다.

ITIL버전은 2000년 V2가 발표되어 정보시스템 IT 운영 프로세스에 가장 많이 반영되었다. 이후 IT 환경 변화와 운영 측면의 요구사항을 모두 반영하기 쉽지 않아 2011년 V3를 신규로 발표하였고, 현재는 2019년 발표된 V4까지 변화되었다. 국내에서는 주로 V2와 V3 기반의 운영프로세스를 적용하여 운영관리 분야 서비스 수준을 관리하고 있다.[8][9]

ITIL V2의 운영업무 프로세스는 비즈니스 요구사항을 만족시키기 위한 IT서비스의 배치이고 방법론이 아닌 Best Practices이다. ITIL 프로세스의 적용은 프로세스에 따른 조직의 변경을 의미하며 서비스를 제공하기 위한 최적의 비용을 제시하는 프레임워크이다. ITIL V2는 서비스 서포트(Service Support) 프로세스와 서비스 딜리버리(Service Delivery) 프로세스로 구분하고 있다. 서비스 서포트 영역은 IT 서비스 사용자가 비즈니스 관련 IT 서비스 품질을 확보하기 위한 매일 발생하는 운영 절차 관련 프로세스를 의미한다.[8] 서비스 딜리버리 영역은 IT 서비스제공자가 비즈니스 고객에게 충분한 지원을 제공하기 위해 필요한 IT 자원설계 및 관리 프로세스를 정의하고 있다.[9] ITIL V2는 IT와 비즈니스 연계관점의 서비스 서포트부문과 서비스 딜리버리부문의 11개 운영 프로세스 영역을 관리하고 ITIL V3는 IT 거버넌스 개념이 포함된 IT서비스 라이프사이클 기반의 운영 프로세스를 정립하였다.[8][9]

ITIL V3는 IT 거버넌스 개념을 추가하여 IT서비스 라이프 사이클 관리 차원의 실질적인 서비스 품질개선과 비즈니스 성과 측정 분야에 구체적이고 현실성 있게 체계화하였다. 세계적으로 인정되는 정보기술 관리를 위한 실천 사례 모음을 제공한다.[10]

ITIL V4는 서비스 가치에 중점을 둔 Service Value System을 기반으로 운영된다. ITIL V4에서 설명되는 34개 프로세스는 고객 및 이해관계자와 함께 가치를 창출하기 위해 필요한 것을 제공한다.[11] 비즈니스 환경에 더 잘 맞도록 유연한 가치중심 운영모델을 통해 기존 프로세스 및 프로젝트 관리방법론, 소프트웨어 개발 운영관리, 생산공정 관리 등의 방법론에 대한 다양한 접근방식을 지원한다. 이러한 프로세스의 범위는 IT산업에 지속해서 영향을 미쳐왔던 ITIL V3 프로세스가 제시하던 관점을 크게 확장했다. 또한, 프로세스에 대한 지침은 모든 조직이 다르다는 것을 인지하고 있으며, 자신의 비즈니스 요구에 적합한 접근방식을 취하기를 권고하고 있다.

ITIL V3 프로세스와 ITIL V4 프로세스 차이는 ITIL V3에서 강조하는 서비스 라이프 사이클 중심의 26개 Process가 ITIL V4에서는 고객에게 서비스를 제공하고 가치를 전달하기 위한 트렌드에 맞는 접근법 관점에서 34개 실천방안으로 대체되었다. 또한, 실천방안에 대한 관점은 모든 조직이 다르다는 것을 인지하고 있으며, 자신의 비즈니스 요구에 적합한 접근방식을 취하기를 권고하고 있다.[11] ITIL V3는 IT서비스의 라이프 사이클에 중점을 두어 도메인별 연계와 지속적 서비스 개선을 강조하고 있다. ITIL V3는 매우 완성된 프레임워크 이였지만, 현재의 클라우드 기반 IT 운영환경을 반영하는 데 한계가 있었다. 클라우드 환경에서는 서비스 관리의 개념이 더욱 강해진다. 릴리즈 주기는 대폭 감소하고, ITSM 각 영역 간 협업요소가 대폭 증가한다.[10] 그러나, 기존의 ITIL V3는 이러한 클라우드 환경에 적절한 가이드를 제공해 주지 못한다. ITIL V3.0은 프로세스의 준수가 생명이지만 클라우드 환경에서의 유기적 업무처리에는 적절하지 못하다. 또한, 복잡해지는 아키텍처 및 사업관리에 대한 실천사례가 부재하다는 점도 존재한다.[10] ITIL V4는 서비스 라이프 사이클에서 서비스 가치사슬 (Service Value Chain)로 근본 사상이 바뀌었다. 즉, 프로세스 중심의 IT 관리에서 조직 상황에 맞는 실무 중심의 IT 관리로의 전환을 뜻한다. 특정 상황에서 불필요한 프로세스를 무조건 수행하는 것이 아니라, 그 상황을 가장 효율적으로 해결할 수 있는 실천 방안을 만들어 해결하면 된다. 또한, 아키텍처 관리, 프로젝트 관리 등 지능정보기술 도입 및 운영을 위한 실행 방안이다.[11]

2.3 서비스수준계약(Service Level Agreement)과 운영수준협약(Operational Level Agreement)[8]

아웃소싱에서 IT 장애가 비즈니스 프로세스에 비용적 손해나 가치적 손해를 끼치는 것은 주요 현안이다. 서비스 이용업체는 아웃소싱업체의 서비스 수준 향상을 위해 인센티브를 통한 동기부여 고취하고, 페널티를 통한 아웃소싱 업체의 지속적인 개선을 요구하는 것이 관리의 핵심과제가 될 것이다.

기업의 비즈니스 활동에 심각한 영향을 주는 정보보안서비스는 SLM(Service Level Management) 프로세스를 통해 서비스 제공업체와 사용업체 간 서비스수준계약(SLA)을 합의하고 이를 달성하기 위해 모니터링, 보고, 리뷰, 개선 등 정상적인 PDCA (Plan-Do-Check-Act) 활동을 통해 서비스의 수준을 유지하고 지속적인 품질향상을 도모하는 일련의 활동을 수행하여야 한다. 이러한 아웃소싱과 같은 외부로부터 서비스를 받는 업체는 SLM프로세스를 구축하고, 서비스수준계약을 지속해서 고도화를 시켜야 한다.[8]

서비스수준계약(SLA)는 IT서비스를 제공하는 업체와 사용자 간의 서비스 수준을 정량적으로 측정하고 서비스 성과를 평가·보상하여 당사자 간 서비스 보증에 대한 합의서로 서비스 이용자에게 제공되는 모든 IT서비스에 대해 체결되며 정히 서명된 것이다.

운영 수준 협약(OLA)은 서비스를 제공하는 업체 간 운영 수준에 대한 상호 대응을 합의하는 것으로 제공되는 서비스가 내부 공급자와 연관된 경우 운영 수준 협약(OLA)을 체결한다. 운영 수준 협약(OLA)은 간단하고 기능적인 문서로서 효과적인 서비스 제공을 위해 각 내부 공급자가 준수해야 할 약정 사항이 기술되어 있다.[8]

외부공급계약(Underpinning Contract)은 외부 공급업체와 체결하는 계약으로서 일반적으로 법률적인 요소와 운영 수준 협약(OLA)에서 볼 수 있는 관리·기술적인 요소를 문서로 만든 것이다.[8]

공공부문은 한 기업이 책임지고 서비스를 제공하는 토탈아웃소싱 계약이 주류이지만 자세히 확인하면 컨소시엄의 형태이거나 여러 업체가 아웃소싱에 참여하는 경우가 많다. 이런 체계의 아웃소싱에서는 관리부서가 SLA 수준 이상으로 운영수준협약(OLA)과 외부공급계약(UC)수준이 반영될 수 있도록 관리되어야 한다.

서비스 제공업체는 사용업체에 약속한 서비스 수준을 만족시키기 위해 운영수준협약(OLA)과 외부공급계약(UC) 항목 등의 하위 성과지표 수준으로 관리되어야 한다.[8] SLA-OLA-UC의 구조는 하위구조의 지표 수준이 상위구조의 지표 수준과 같거나 높아야 하며 상위구조의 수준을 하위구조에서 보증해 주어야 한다. SLA 성과지표와 연계할 수 없는 하위 운영 수준 협약(OLA) 또는 외부공급계약(UC)계약 수준이 존재할 경우 서비스 이용업체에 제공되는 SLA 서비스 수준은 보증될 수 없다.

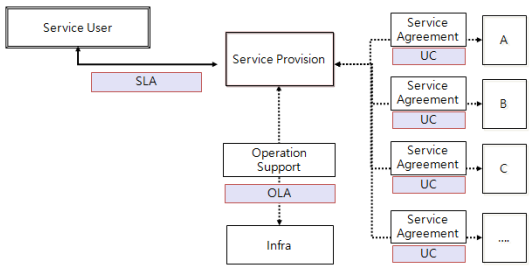

Fig. 1. SLA Structure

본 논문에서는 이런 구조 중에서 운영 수준 협약(OLA)성과지표를 통한 서비스 수준을 관리하는 성과지표를 선정하여 SLA 성과지표로 치환하여 평가 보상하는 방안을 제공할 것이다. 본 연구에서는 〈그림 1〉과 같이 SLA 구조를 제시한다.

III. 제안 방법론

3.1 SLA방법론

ITIL에서 제공하는 운영 프로세스는 표준을 제시하는 것이 아니라 베스트 프랙티스 모음집으로 ITSM도입을 위한 지침으로 활용되고 있다. 기업은 환경에 따라 프로세스 도입 및 개선 작업을 방법론을 정의하여 진행하여야 한다.[8][9]

운영 관리는 점진적 향상으로 서비스의 목표와 수행 결과는 정량적인 지수로 표시하여 해당 관련자들의 동일한 관점을 유지하는 것이 필요하다.

SLA 방법론은 정보보안 지침과 운영프로세스와 연동하는 서비스 수준 계약을 최적화하여 개발 할 수 있도록 SLA 개발하고 적용한다. 본 연구에서 SLA 적용방법론 단계를 계획·분석·설계·개발·계약·적용·통제 단계로 정의하는 방법을 제시한다.

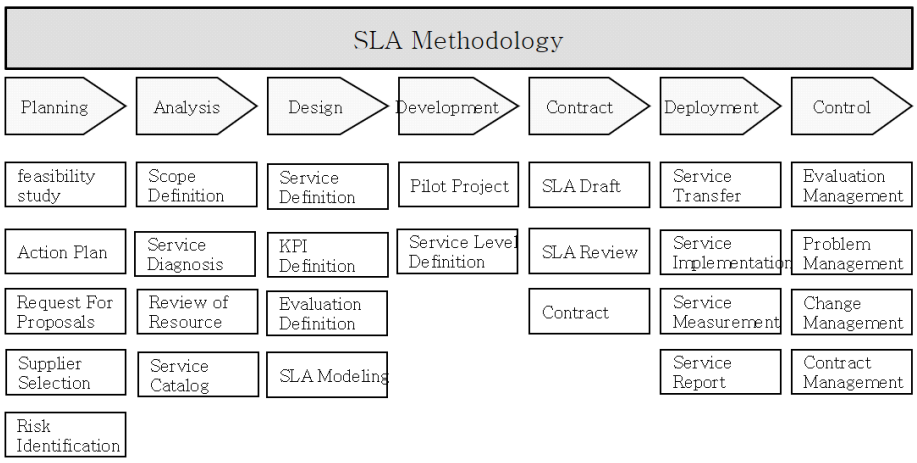

Fig. 2. SLA Methodology

3.2 정보보안 서비스

일반적으로 IT서비스는 IT 환경을 분석하여 서비스 유형별로 분류하고 정의한다. IT서비스는 "비즈니스 프로세스를 가능하게 하는 하나 또는 많은 IT시스템의 결합"으로 이루어진다.[8] 정보보안 서비스는 보안을 위한 프로세스를 가능하게 하는 보안시스템의 결합 형태로서 애플리케이션, 소프트웨어, 하드웨어 등과 같은 IT 자원으로 구성된다.

이러한 분류는 향후 구성관리 프로세스의 항목으로 진행하며, SLA 성과지표 설계의 기준이 된다. 또한, 정보보안 서비스 분류 레벨은 서비스 이용업체에 제공하는 보안 서비스 리포팅의 관리 단위가 된다. 〈Fig. 3〉과 같이 정보보안 구성요소를 제시한다.

본 논문에서는 정보보안 서비스를 컨설팅 서비스, 인프라 운영 서비스, 보안관제 서비스로 나눈다.

컨설팅 서비스는 조직의 규정 준수, 보안 분야 위험 관리에 더 효과적으로 충족할 수 있는 대책을 수립하여 최적의 정보보안시스템을 설계하기 위한 서비스를 제공한다. 준비 및 설계부터 구축, 운영, 최적화까지 실행 전반에서 고객의 고유한 문제를 해결하고 고객의 비즈니스 목표를 달성하는 데 유용한 정보보안 관리체계 및 요소 기술을 제공한다. 또한, 프로젝트를 요구 사항에 일치하기 위해 모든 문제 요인을 식별하고 최소화하기 위한 해결방안 및 우선순위를 분석한다.

인프라 운영 서비스는 물리적인 또는 소프트웨어 방어 도구를 이용해 기반 IT 인프라에 승인되지 않

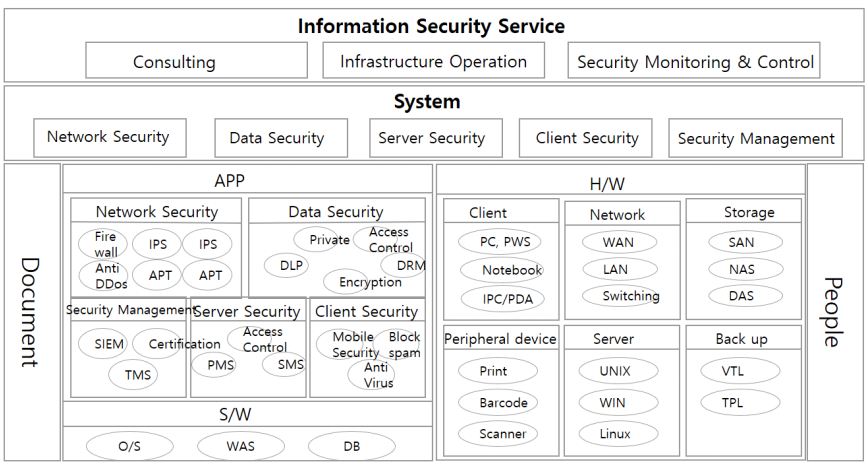

Fig. 3. The Configuration Items of Information Security

은 액세스나 오용, 오동작, 수정, 파괴, 부적절한 노출 등으로부터 보호하는 프로세스이다. 급변하는 IT 환경변화에 대응하여 서버의 내·외부 시스템보안을 다루고 보다 안전하게 IT 인프라를 운영하여 비 인가된 외부 위협으로부터 컴퓨터와 사용자, 그리고 프로그램이 승인된 핵심 기능을 안전한 환경에서 수행할 수 있도록 운영한다.

보안관제 서비스는 기업의 일상적인 정보보안 업무를 효율적으로 수행하기 위해 기업이 보유한 보안 시스템을 기반으로 24×365동안 모니터링, 정책설정, 침입시도에 대한 탐지, 분석, 대응 등과 같은 보안 활동을 지속해서 수행하는 서비스이다.

또한, 비 인가된 침해사고에 대한 신속한 대응을 통해 피해를 최소화하고 즉각적인 보고를 통해 유사한 공격에 대한 대응책을 수립한다.

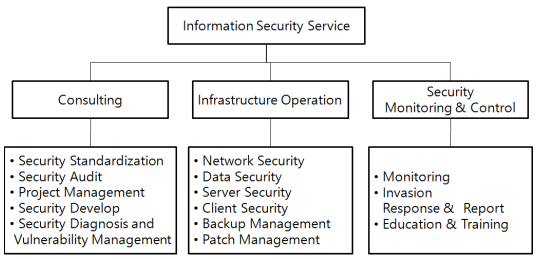

Fig. 4. The classification of Information Security Service

3.3 정보보안SLA 성과지표 선정

정보보안 SLA 성과지표는 타 연구에서 도출된 보안 SLA 성과지표와 보안 서비스 수준 향상을 위해 유관 운영프로세스에서 파생되는 측정지표를 통해 선정된다. 보안서비스는 IT운영프로세스를 공유하면서 운영되어 진다.

첫째, 정보시스템 운영관리지침과 ITIL 프로세스를 기반으로 정보보안 서비스 향상을 위한 운영프로세스를 선택한다. 운영프로세스의 비즈니스 요구사항을 만족시키기 위한 주요 성과지표를 도출한다. 현재 공공부문에서 주로 사용되는 프로세스는 ITIL기반의 운영 프로세스이다.[8][9][12]

둘째, 정부와 공공기관에서 제공하는 보안 SLA 효율적 운영방안 개발"(KISA), 사단법인에서와 정부 기관 "정보보안 가이드라인"을 활용하여 기업별 환경에 따라 적용 여부를 확인하고 운영프로세스 강화를 위한 성과지표를 혼합하여 성과 지표 Pool을 형성한다.

Table 2. The comparison of Operation Process

	The operation management guidelines of Information system	ITIL
Process	Configuration Management	Service Desk
	Change Management	Incident Management
	Operation Statement Management	Problem Management
	Capacity Management	Change Management
	Performance Management	Release Management
	Incident Management	Configuration Management
	Problem Management	Service Level Management
	Backup Management	Capacity Management
	Request Management	Continuity Management
	Information System Room Management	Availability Management
	Service Level Management	Financial Management
	Financial Management	

셋째, 운영관리지침과 운영 프로세스에서 파생되는 성과지표와 공공기관 및 사단법인 연구개발보고서의 성과지표를 기준으로 설문조사를 수행한다.(Appendix 1)

모든 성과지표는 관련 업무를 수행하는 전문가의 설문조사를 통해 선정되었다. 정보보안 SLA 성과지표를 선정하기 위해 공공부문 실무자, 관리자 그리고 공공사업 PM 20명을 대상으로 조사하였다. 설문 문항은 5점 척도를 사용하였고 도출된 SLA 성과지표의 중요도를 조사하였다. 평균점수는 100점 환산으로 82.05를 기록하였다. 모든 평가자는 서비스수준계약에 대한 이행을 경험함과 동시에 서비스수준계약에 대한 지식을 보유하고 있는 전문가이다. 본 논문에서 설문조사를 통해 중요도 90점 이상의 항목에 대해 정보보안 SLA 성과지표로 선정하였다. 설문조사 항목은 운영 수준 협약(OLA) 성과지표로 구성되었으며, 운영 수준 협약 항목을 서비스 관점으로 분류한 SLA 항목으로 분류하였다.(Appendix 2)

모든 운영관리를 위한 프로세스는 서비스수준관리 프로세스로 입력되어 합의된 SLA 항목에 대한 측정치를 제공한다. 서비스수준관리 프로세스는 고객의 입장에서 작성된 SLA 리포팅 및 모니터링에 대한 내용이 담겨있는 프로세스를 관리한다.

이러한 성과지표 적용은 정보보안 관리 분야의 특성을 반영한 후, 일정 부문 현행화 등을 통해 적용이 가능할 것이라고 본다.

3.4 정보보안 SLA성과지표 정의서

정보보안 성과지표 정의는 정보보안 정책 수립 및 성과평가를 위한 합리적인 의사결정을 내릴 수 있도록 수치화하는 도구로 조직별 정보보안 현황을 객관적 기준에 따라 평가할 수 있는 체계를 의미한다. 기업은 주기적인 성과지표 측정을 통해 자사의 정보보안 현황분석 및 추이 분석이 가능하며 이를 통한 정보보안 전략을 수립하는 자료로 활용한다.(정보보호 성과지표, 2013) 성과지표는 객관성이 확보되도록 설계되어야 하며 합리적인 결과를 제공해야 하며 조직의 특성이 반영된 성과지표를 선정해야 함과 동시에 회사의 목표와 연계성을 가져야 한다.

정보보안 성과지표에 대한 구체적인 측정내용은 성과지표정의서로 표현되며 서비스 수준 측정을 위한 지표 정의, 계산방식, 측정 방법, 수준 평가 기준 및 서비스 수준 평가의 전제 사항 등을 기술한다. (Appendix 3)

3.5 정보보안 SLA 서비스수준 평가

본 논문에서 설문조사 항목은 운영 수준 협약(OLA) 차원의 성과지표이며 서비스 제공업체 간 상호 관리하기 위한 협약이다. 운영프로세스 강화 및 지침 기반의 성과지표는 서비스 이용업체 관점에서 이해 할 수 있는 SLA 성과지표로 변경되어야 한다. 정보보안 SLA는 컨설팅 부문, 보안관제 부문, 인프라 운영 부문으로 분류되고 보안관제와 인프라 운영 성과지표는 정보보안을 구성하는 IT 인프라 분류에 의해 네트워크, 서버, 클라이언트보안으로 나누고 서비스 성과지표로 포함한다.

분류된 정보보안시스템은 중요도에 따른 가중치를 적용하고 운영수준협약(OLA)성과지표의 가중치를 맵핑하여 SLA 성과지표로 표현된다.

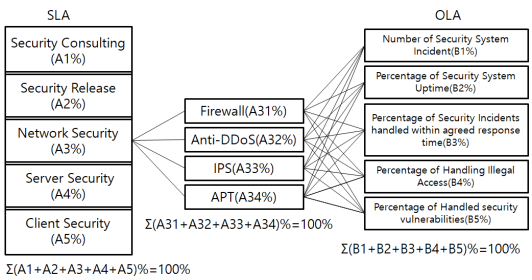

Fig. 5. The Structure of SLA KPI

정보보안시스템은 긴급도(Agency)와 영향도(Impact)에 따라 업무중요도를 분류한다. 긴급도는 장애 발생 시 기업 손실 비용 크기와 대외신뢰도에 영향을 주는 것이며, 영향도(Impact)는 장애 발생 시 비즈니스 프로세스의 중단 범위를 의미한다. 더불어, 시스템 유지보수의 난이도를 추가하여 정보보안 시스템 중요도를 결정한다.

Table 3. The Weight Percentage of KPI

Service	Rate	OLA KPI	Survey Score	Percentage of Weight
Security Consulting	100%	Percentage of Handled security vulnerabilities	99	0.594
		Percentage of Privacy Encryption	95	0.277
		Number of mock hacking vulnerabilities found	90	0.129
Infrastructure Operation	100%	Percentage of Handling Illegal Access	98	0.271
		Persentage of Security Patch handled within agreed response time	97	0.188
		Persentage of handled Operation Systems' Patch	97	0.188
		Percentage of Account Check	96	0.133
		Number of Security System Incident	94	0.102
		Percentage of Security System Uptime	93	0.069
		Percentage of Back-up Success	90	0.051
Security Monitoring&Control	100%	Persentage of Security Incidents handled within agreed response time	97	0.311
		Persentage of Vaccine installation	97	0.311
		Percentage of Handling vulnerabilities	95	0.189
		Percentage of unauthorized software installations	92	0.111
		Percentage of Receive Spam Mail	91	0.078

운영 수준 협약(OLA)항목은 설문조사의 점수에 따라 중요도 가중치 비율을 산정한다. SLA 분류별 운영수준협약(OLA)항목의 비중은 설문조사 시 절대평가 점수를 AHP쌍대비교방식을 활용하여 정보보안 서비스별 성과지표 가중치를 산정하였다.

SLA 적용은 인센티브와 페널티 조항을 넣어 점진적인 서비스 수준 향상을 지향한다. 측정된 성과지표 측정치를 분석하여 서비스 수준 평가를 위한 기대치와 최소치를 정의한다.

첫째, 정보보안 SLA 성과지표에 대한 12개월 이상의 데이터가 있으면 서비스 기대 수준은 측정 데이터의 평균으로 하고 서비스 최소수준은 측정데이터의 최소치로 한다.

둘째, 성과지표의 측정된 데이터가 없으면 객관성을 보유한 제삼자의 권고안이나 계약 당사자 상호 간의 협의한 값을 사용한다. 성과지표에 대한 상호 간 의상호간의 협의가 되지 않을 때에는 다음과 같은 운영방안을 제시한다.

성과지표 항목이 추가되면 계약 당사자는 60일 이내에 측정을 시작하고 12개월 데이터가 축적되면 측정치의 평균과 최소치를 사용한다.

적용 필요성이 긴급한 경우에는 1개월의 데이터가 없으면 그달의 서비스 수준은 11개월 중 최고 수준으로 적용한다. 2개월 이상의 데이터가 없을 때는 1개월은 최고 수준을 사용하고 나머지 개월은 최고 수

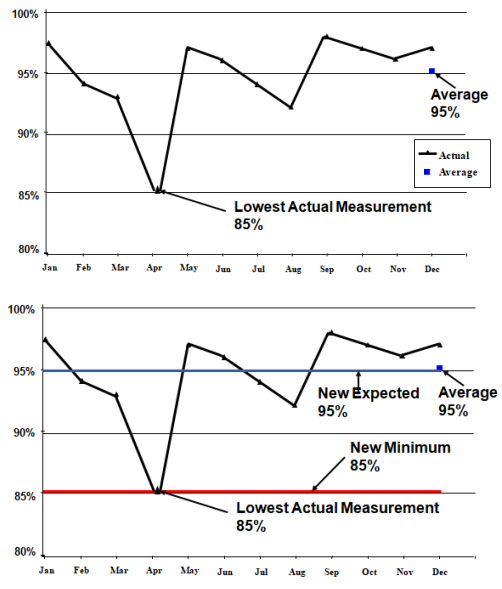

Fig. 6. The Definition of SLA KPI Standards

준과 100%의 차이의 20%를 곱한 값을 사용하여 기대 수준과 최소 수준을 결정한다.

계약 기간에 1년 경과 이후에 새로운 기대 수준과 최소수준은 당사자 간 합의에 따라 진행한다. 합의가 되지 않을 경우 기준 선정 룰을 적용한다.

기대 수준은 기 측정치의 평균을 적용하고 이전 수치보다 낮을 경우 이미 적용된 기대 수준을 유지한다. 최소수준은 기대 수준과 최소수준 사이의 기 측정치의 평균과 최소수준의 중간값을 선정하여 점진적인 서비스 향상을 도모한다.

비율(%)로 표현되지 않은 정보보안 SLA 성과지표는 상위 4개의 측정치의 평균을 기대 수준으로 설정하고 하위 4개의 평균을 최소수준으로 설정한다. 계약 기간 내 기대 수준과 최소 수준은 하향하지 않는다. 범위 내 측정치의 평균이 낮으면 이미 설정된 기준을 적용한다.

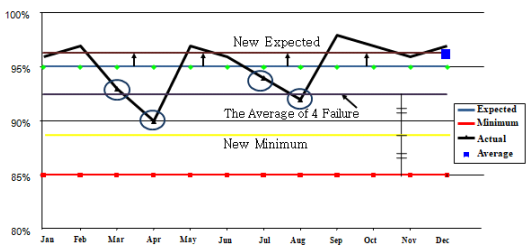

Fig. 7. The Renegotiation of SLA KPI Standards

성과지표가 절대 값 100점이나 100%에 3개월 이상 수렴하는 경우는 최고의 서비스 받는 것을 의미하며, 향후 성과지표 재설정 시 특정 기간 제외되어야 한다.

3.6 정보보안 SLA 성과체계

계약 상대자 간 제공되는 서비스 수준을 정량적으로 측정하여 서비스 성과를 평가한다는 동의에 따라 일정 수준의 서비스를 명시한다. 적절한 서비스 제공을 보장받기 위해 성과측정에 따른 보상(인센티브)과 제재(페널티) 정책이 제공된다.

성과측정은 IT 아웃소싱 업체 선정 시 업체가 제시한 수준을 평가하는 기준으로 활용 가능하며 서비스에 대한 비용을 산정할 때 매우 중요한 역할을 한다. SLA에 대한 정확한 수치와 직관적인 성과 측정, 이에 따른 비용 지급은 서비스 수준 향상을 높인다. 성과측정에 따른 인센티브, 페널티 제도 도입이 필요한 이유로는 서비스 중심으로 비용을 지급하기 때문에 인력 가동률 최적화로 불필요한 인력 사용을 최소화 할 수 있다.

항목별 평가는 영업 이익률을 고려하여 서비스 제공업자의 최소 이익을 보장하는 범위에서 가중치에 의한 보상으로 산정되어야 한다.

항목별 성과 평가는 세 단계로 구성되며 기대 수준을 상회하여 인센티브가 보장되는 목표 초과단계, 기대치와 최소치의 중간을 유지하는 목표달성단계, 최소치를 하회하여 페널티가 부가되는 목표 미달로 구분된다.

항목별 인센티브와 페널티 부여는 월별로 측정되며, 최소치 이하로 측정된 경우와 년 기준 실제 서비스 수준이 4개월 이상 기대치를 초과하지 못할 때도 페널티를 부여한다. 그러나, 계약 기간 동안 서비스 수준의 평균이 기대치를 초과하면 페널티 금액은 소멸한다.

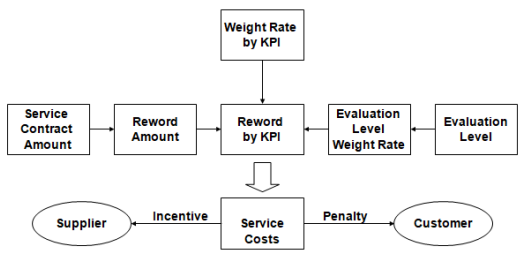

Fig. 8. Evaluation Process

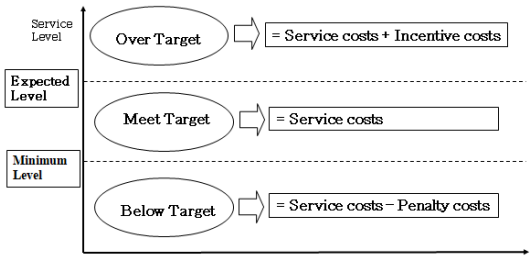

Fig. 9. The Steps of KPI Evaluation

IT 비용은 하드웨어, 소프트웨어, 유지보수 및 운영비, 외부공급계약(UC) 비용으로 구분할 수 있다. 계약기관은 기본 2년에서 서비스 제공 수준에 따라 1년 연장계약으로 한다. 하드웨어는 5년을 기준으로 균등 상가법으로 감가한다. 유지보수 인건비는 계약기간 동안 불변이며, 외부공급계약(UC)비용은 하드웨어 비용 감가로 인해 매년 하향 조정 되고 있다. 유지보수 인력 수는 시간이 지날수록 숙련도는 증가하나, 노후화되는 하드웨어를 고려한다면 계약 기간 동안 변화가 없다.

국내 IT 유지보수 및 운영에 대한 금액 책정은 최저가 공개 입찰 방식으로 입찰가액은 운영 인력 비용 및 장비 유지보수를 위한 외부공급계약비, 유지 활동을 위한 제경비, 고객사 서비스 유지를 위한 인력의 기술료 등이 포함되어 있다. 정보보안 IT 장비는 서비스 중요도에 따라 분류 하고 있으며, Man

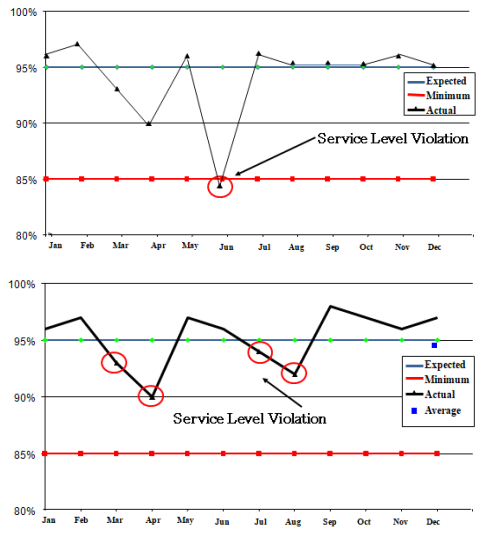

Fig. 10. Penalty Rule

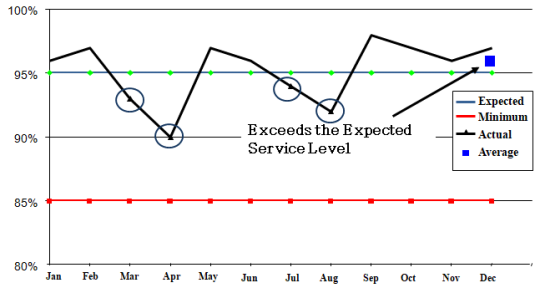

Fig. 11. Penalty Exception Rule

Month 대가 방식의 기준은 정보 시스템 산업 진흥원의 SW 기술자 노임단가의 평균 단가 적용을 받고 있다.

국내 아웃소싱 비용에서 운영 인력 비용과 제경비 합의 20%~40%를 기술료로 산정한다. 서비스 제공 업자의 이익을 보장하면서 서비스 수준 향상을 위해 서비스 인센티브는 기술료의 영업이익 금액으로 인센티브와 페널티의 비율을 차등 부과한다. 최대 인센티브 금액은 기술료 총액의 50% 이내로 조정되어야 하고 최대 페널티 금액은 기술료 총액의 40%로 한정한다. SLA 항목별 단가에 대해 기술료와 가중치 비율을 활용하여 인센티브 금액 및 페널티 금액을 산정한다.

1년 단위의 SLA에서
월 항목별 인센티브 금액
$= (\Sigma\ N1 + N2 \ldots + Nn) \times r \times I \times w / 12$

월 항목별 페널티 금액
$= (\Sigma\ N1 + N2 \ldots + Nn) \times r \times 80\% \times P \times w / 12$
N : SLA 항목별 운영 인력 비용, r : 기술료 비율(%),
I : 인센티브 비율(%), P : 페널티 비율(%),

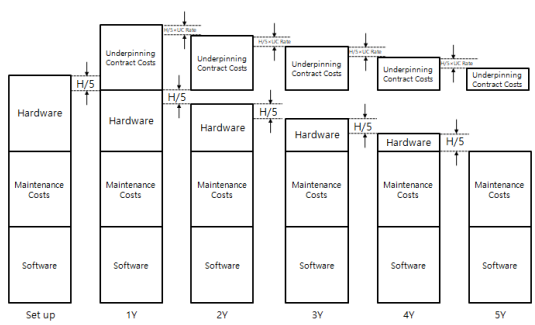

Fig. 12. IT Costs in Public Sectors

w : 성과지표 가중치 비율(%)

위와 같이 산정한다. 페널티 금액의 최대치는 서비스제공업자의 기본적 이익을 보장하기 위해 최대 인센티브 금액의 80%를 최대치로 한다.

IV. 결 론

현재 국내 공공부문 정보시스템 운영 관리는 조직의 정보 보안 환경과 무관하게 일반적인 운영 프로세스 구축으로 수행되고 있다. IT 주변 환경의 변화에 따른 중요도의 차이에 따라 지속적인 개선을 통해 조직에 최적화된 프로세스로 진화되어야 한다. 끊임없이 Plan-Do-Check-Act 활동으로 운영 프로세스 범위의 확장과 기본 되는 운영 프로세스의 고도화에 집중해야 한다.

과거 정보 보안은 IT의 내부 비즈니스를 보호하는 운영 프로세스에 지나지 않았지만 현재에는 IT와 운영 프로세스를 공유하는 다른 비즈니스 영역으로 중요성이 확대되었다. 이런 현재의 상황에 따라 정보 보안은 새로운 성과 지표를 통해 기존 IT SLA와 구별되는 서비스 수준 계약을 만들어야 한다.

현재 공공부문 및 일반 기업에서 IT 측면의 SLA가 활성화되어 있다. 조직에서 정보 보안에 대한 관리 영역이 IT 관리 영역과 분리되고 조직의 달성 목표가 상이함에 따라 본 논문에서는 정보 보안 강화를 위한 SLA 성과 지표 선정을 하고 성과체계 적용 방안을 제시하였다.

실제 조직에서 정보 보안 업무를 수행함과 동시에 SLM 프로세스에서 SLA을 구현하고 관리하는 담당자를 중심으로 설문 조사를 통해 실 환경에서 사용될 수 있는 성과 지표를 선정하였다. 이 성과 지표를 평가할 수 있는 객관적인 적용 방안을 제시함으로 참고 또는 활용이 가능하다.

특히, 성과체계 적용 방안은 실제 사례를 중심으로 공공기관 담당자와 SI 업체 관리자 및 유관 인력과의 협업을 통해 수행된 연구이다. 향후, 정보 보안 SLA 부문이 공공부문 및 일반 기업에 유용하게 활용될 수 있다고 판단한다.

References

[1] Choi, Yun-Ho. "A IT Service Management Performance Model Based on Val IT for IT Governance." Proceedings of the Korea Information Processing Society Conference. Korea Information Processing Society, pp.1724-1727, Nov. 2012

[2] Park, Chul-Han, Sang-Soo Kim, and Hoh In. "A Selection Methodology for SLA Evaluation Factors with End-user Perspective." Proceedings of the Korea Information Processing Society Conference. Korea Information Processing Society, pp.495-498, Nov. 2006

[3] Sim, Hyun-bo. "From Information Security To Syber Security." RESEAT Monitoring Report, 2012.

[4] Lee, Byoung-Chol, and SungYul Rhew. "The Maintenance Cost Estimation Model for Information System Maintenance Based on the Operation, Management and Service Metrics." Journal of The Korea Society of Computer and Information 18(5), pp.77-85, May. 2013

[5] Kang, Un-Sik, Kyoung-Han Bae, and Hyun-Soo Kim. "A Cost Optimization Model of IT Operation Service by Improving Service Request Management Process." Journal of Information Technology Services 6.3, pp.87-110, Dev. 2007

[6] Park, WonIl, and MyongSoon Park. "Cloud computing billing system associated with SLA." Proceeding of Korea Computer Congress 2013, pp.854-855, Jun. 2013

[7] Standard, Australian. "ISO/IEC27002." Informationtechnology-security techniques-code of practice for information security controls,(AS ISO/IEC 27002: 2015). 2015.

[8] ITIL, "Service Support", The Stationery Office, 2001

[9] ITIL, "Service Delivery", The Stationery Office, 2001

[10] Hwang Kyung-tae and Nam Gi-chan.“Foundation of IT Service Management Based on ITIL V3”, 2008
[11] Claire Agutter. “ITIL Essentials Foundation Essentials ITIL 4 Edition”, ITIL, 2020
[12] National Information Society Agency. “The Operation Management Guideline of Information System”, 2005
[13] Jo, Yeon-ho, et al. "A Study on Policy for cost estimate of Security Sustainable Service in Information Security Solutions." Journal of the Korea Institute of Information Security & Cryptology, 25(4), pp905-914, Aug. 2015
[14] Shin, Sung-Jin, Sung-Yul Rhew, and Yoo-Ri Kim. "A case study on selection and improvement of sla evaluation metrics." The KIPS Transactions: PartD 16.4, pp.541-548, Aug. 2009
[15] KISA, “Development of efficient operation plan of security SLA for security service.” pp.99-145. 2010
[16] Lee, E. J. "A Study on the Operation of ITSM for Small Scale IT Department." Journal of Human Computer Interaction 2011.1 (2011): 12-13.
[17] Kim, Dong-Soo, and Hee-Wan Kim. "A Study on the Audit Model of Outsourcing Operation based on Availability Metrics in perspective of Service Level Agreenment." Journal of digital convergence 13.7, pp.183-196, Jul. 2015
[18] Rhew, Sung-Yul, Sung-Jin Shin, and Yoo-Ri Kim. "A Study on Selection and Improvement of SLA Evaluation Metrics Using IT Maturity Model." Journal of Information Technology Services 8.4, pp141-150, Dec. 2009

〔Appendix 1〕 The Survey of Information Security KPI

Process	Key Performance Indicator		Process	Key Performance Indicator	
Request Management	Percentage of Incidents closed by the Service Desk without reference to other levels of support	REQ_1	Capacity Management	Percentage of Preventive inspection	CAP_1
	Customer Satisfaction	REQ_2		Percentage of Inspection	CAP_2
Incident Management	Number of Server Incident	INC_1		Percentage of Resource Threshold Compliance	CAP_3
	Number of Network Incident	INC_2	Continuity Management	Percentage of Server Redundancy	CNT_1
	Number of Security System Incident	INC_3	Backup Management	Percentage of Back-up Success	BAC_1
	Persentage of Incidents handled within agreed response time	INC_4		Percentage of Backup Recovery Training	BAC_2
	Tatal numbers of repetitive Incidents	INC_5		Percentage of Backup failure	BAC_3
	Tatal numbers of Incidents	INC_6	Security Management	Percentage of Connection Blocking	SEC_1
Problem Management	Persentage of handled problem	PBM_1		Percentage of Handled security vulnerabilities	SEC_2
Change Management	Persentage of Change handled within agreed response time	CHA_1		Percentage of Account Check	SEC_3
Release Management	Persentage of Security Patch handled within agreed response time	REL_1		Persentage of Security Incidents handled within agreed response time	SEC_4
	Persentage of handled Operation Systems' Patch	REL_2		Percentage of Handling Illegal Access	SEC_5
	Persentage of Vaccine installation	REL_3		Percentage of unauthorized software installation	SEC_6
Configuration Management	Percentage of The accuracy of Configuration Information	CON_1		Percentage of Receive Spam Mail	SEC_7
Availability Management	Percentage of Server Uptime	AVA_1		Percentage of Privacy Encryption	SEC_8
	Percentage of Network Uptime	AVA_2		Number of mock hacking vulnerabilities found	SEC_9
	Percentage of Security System Uptime	AVA_3		Percentage of Handling vulnerabilities	SEC_10
	Response Time	AVA_4			

REQ_1	REQ_2	INC_1	INC_2	INC_3	INC_4	INC_5	INC_6	PBM_1	CHA_1	REL_1	REL_2	REL_3	CON_1	AVA_1	AVA_2	AVA_3	AVA_4
1	1	3	3	5	2	3	2	2	2	5	5	5	5	2	2	5	2
1	1	2	2	5	1	3	1	3	1	4	4	4	3	1	1	5	1
1	1	1	1	4	1	1	1	2	1	5	5	5	2	1	1	5	1
3	3	2	2	4	2	2	2	2	2	4	4	4	2	1	1	4	2
2	5	2	3	4	5	1	1	2	1	5	5	5	2	3	3	4	1
2	2	4	4	5	4	2	4	4	4	5	5	5	4	4	4	5	2
3	3	4	4	5	4	3	4	4	4	5	5	5	4	4	4	5	3
2	2	4	4	5	4	3	4	4	4	5	5	5	5	5	5	5	3
4	4	4	4	5	5	5	5	4	5	5	5	5	4	4	4	4	4
5	5	3	3	3	3	5	3	3	5	5	5	5	5	3	3	4	3
5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
3	2	5	3	5	5	3	5	4	4	5	5	5	5	3	3	5	4
1	3	5	5	5	5	5	5	5	4	5	5	5	5	4	4	5	4
5	5	3	3	4	5	3	5	2	3	5	5	5	5	5	5	5	3
3	3	4	4	5	5	5	5	5	5	5	5	4	5	4	4	5	4
3	4	5	5	5	5	4	5	4	4	5	5	5	5	4	4	5	3
5	2	3	3	5	4	3	3	5	4	5	5	5	5	4	4	4	3
4	3	4	3	5	4	3	4	5	4	5	5	5	4	3	4	4	3
3	3	5	5	5	5	5	4	5	3	4	4	5	4	4	4	4	4
4	5	4	4	5	5	5	3	5	2	5	5	5	3	3	3	5	3
60	62	72	70	94	79	69	71	75	67	97	97	97	82	67	68	93	58

CAP_1	CAP_2	CAP_3	CNT_1	BAC_1	BAC_2	BAC_3	SEC_1	SEC_2	SEC_3	SEC_4	SEC_5	SEC_6	SEC_7	SEC_8	SEC_9	SEC_10
3	4	3	3	4	4	4	5	5	5	5	5	5	5	5	5	5
3	2	2	2	4	4	3	5	5	5	5	5	4	5	5	4	5
2	2	1	1	5	5	5	5	5	5	5	5	5	5	5	5	5
3	3	2	2	4	4	4	4	5	4	5	4	4	5	5	4	4
2	2	1	1	5	5	5	5	5	5	5	5	5	5	4	5	5
4	4	4	4	4	4	4	4	5	5	5	5	5	5	5	5	5
4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5	5
4	5	4	4	5	4	4	5	5	5	5	5	5	4	5	5	5
3	5	3	3	5	3	5	5	5	5	5	5	5	3	5	5	5
5	5	5	4	5	5	5	5	5	5	5	5	5	4	5	5	5
5	5	4	5	4	5	5	4	5	5	5	5	5	5	5	5	5
4	4	4	4	4	3	5	5	5	5	5	5	4	3	5	4	5
3	3	3	3	3	3	3	3	5	5	5	5	5	5	3	4	5
4	4	4	5	5	5	3	3	5	5	5	5	5	5	4	5	5
5	5	4	4	5	5	4	4	5	4	5	5	5	4	5	5	5
5	4	4	4	5	5	4	4	5	5	4	5	4	4	3	4	4
5	5	4	3	4	4	4	3	5	5	4	5	4	5	4	3	4
5	5	5	4	5	4	4	4	5	4	5	5	4	5	4	4	4
5	5	3	4	5	5	5	5	5	5	5	5	4	5	4	4	5
79	81	69	69	90	86	85	87	99	96	97	98	92	91	90	90	95

〔Appendix 2〕 SLA KPI Survey Results

Process	Key Performance Indicator		Process	Key Performance Indicator	
Request Management	Percentage of Incidents closed by the Service Desk without reference to other levels of support	REQ_1	Capacity Management	Percentage of Preventive inspection	CAP_1
	Customer Satisfaction	REQ_2		Percentage of Inspection	CAP_2
Incident Management	Number of Server Incident	INC_1		Percentage of Resource Threshold Compliance	CAP_3
	Number of Network Incident	INC_2	Continuity Management	Percentage of Server Redundancy	CNT_1
	Number of Security System Incident	INC_3	Backup Management	Percentage of Back-up Success	BAC_1
	Persentage of Incidents handled within agreed response time	INC_4		Percentage of Backup Recovery Training	BAC_2
	Tatal numbers of repetitive Incidents	INC_5		Percentage of Backup failure	BAC_3
	Tatal numbers of Incidents	INC_6	Security Management	Percentage of Connection Blocking	SEC_1
Problem Management	Persentage of handled problem	PBM_1		Percentage of Handled security vulnerabilities	SEC_2
Change Management	Persentage of Change handled within agreed response time	CHA_1		Percentage of Account Check	SEC_3
Release Management	Persentage of Security Patch handled within agreed response time	REL_1		Persentage of Security Incidents handled within agreed response time	SEC_4
	Persentage of handled Operation Systems' Patch	REL_2		Percentage of Handling Illegal Access	SEC_5
	Persentage of Vaccine installation	REL_3		Percentage of unauthorized software installations	SEC_6
Configuration Management	Percentage of The accuracy of Configuration Information	CON_1		Percentage of Receive Spam Mail	SEC_7
Availability Management	Percentage of Server Uptime	AVA_1		Percentage of Privacy Encryption	SEC_8
	Percentage of Network Uptime	AVA_2		Number of mock hacking vulnerabilities found	SEC_9
	Percentage of Security System Uptime	AVA_3		Percentage of Handling vulnerabilities	SEC_10
	Response Time	AVA_4			

〔Appendix 3〕 SLA KPI Definition

Metric		Percentage of Security System Uptime		
Definition		The percentage of time that the entire IT service is fully operated according to the quality level		
Object		Network Security System, Server Security System, Client Security System		
Formula		(1-Total Incident Time/ The planned Service Time)×100%		
Level Definition	Expected Level	Network Security System	Server Security System	Client Security System
		98.43	**99.80**	**98.92**
	Minimum Level	Network Security System	Server Security System	Client Security System
		98.00	**99.40**	**97.00**
Measurement Standard	Source Data	The Incident Report		
	Standard	Service hours excluding Incident time		
	Measure	Calculate the actual service uptime by summing the unplanned service downtime measured du ring the planned service uptime period and subtracting it from the planned service uptime.		
	Cycle	Monthly meeting		
Report plan		• Service utilization rate calculated on a monthly basis		
Condition		• Calculated as service interruption in case of simultaneous clustering failure • Calculated as service interruption in case of DB server failure		

〈저자소개〉

정 재 호 (Jae Ho Jeong) 정회원
2019년 9월~현재: 고려대학교 정보보호대학원 사이버보안학과 석사과정
〈관심분야〉 네트워크보안, 시스템보안, ITSM, SLA

김 휘 강 (Huy Kang Kim) 종신회원
1998년 2월: KAIST 산업경학학과 학사
2000년 2월: KAIST 산업공학과 석사
2009년 2월: KAIST 산업 및 시스템공학과 박사
2004년 5월~2010년 2월: 엔씨소프트 정보보안실장. Technical Director
2010년 3월~2014년 12월: 고려대학교 정보보호대학원 조교수
2015년 1월~2020년 2월: 고려대학교 정보보호대학원 부교수
2020년 3월~현재: 고려대학교 정보보호대학원 교수
〈관심분야〉 온라인게임 보안, 자동차 보안, 침입탐지시스템, 네트워크 보안