ISO22301 기반 비지니스 연속성 증대를 위한 효율적인 정보시스템 운영감리 점검항목 설계

주 낙 완* · 김 동 수** · 김 희 완***

목 차

요약

본 논문은 빅데이터, 사물인터넷, 인공지능 등 정보기술의 발전과 더불어 더욱 중요해진 정보시스템의 비즈니스 연속성 증대를 위한 운영감리 개선에 관하여 연구하였다. 다양한 서비스와 데이터 그리고 산업이 융합되는 4차 산업시대에 도래하고 있는 현재 정보시스템의 운영관리와 감리지침은 기존의 범용적 정보시스템 패턴에 근거해 대응하고 있어 이에 대한 개선이 요구된다. 정해진 시간에 정해진 서비스의 제공이 기업 및 국가의 생존과 연결되고 핵심 요소로 작용하고 있으므로 비즈니스 연속성 관리차원에서 정보시스템의 서비스 중단 피해를 최소화하고 안정된 서비스 수준을 제공하기 위한 운염감리의 최적화된 방향성과 점검항목을 적용하는 연구가 필요하다. 이를 위해 정보시스템의 운영감리에서 제시하는 점검항목을 ISO 22301 에서 제공하는 PDCA 단계별 내용과 8대 자원 요구사항을 접목하여 도출하였다. 점검항목의 도출기준에 따라 비즈니스 연속성 증대 관점에서 정보시스템 운영감리의 개선된 점검항목과 검토항목 그리고 운영감리 중 점검해야 할 산출물을 예시로 운영감리 점검항목을 도출하였다. 점검항목으로는 서비스 연속성 관리를 위한 운영감리 개선 점검항목과 성능, 가용성 관리를 위한 운영감리 개선 점검항목으로 구분하여 제안하였다. 제안한 점검항목의 적합성에 대한 IT전문가들의 5점 척도 설문 결과 평균 4.63으로 나타나 적합하다는 결론이 도출되었다.

표제어: 비지니스 연속성, 정보시스템 운영감리, 점검항목, ISO22301, PDCA

접수일(2019년 5월 9일), 수정일(1차: 2019년 6월 15일), 게재확정일(2019년 6월 24일)
※This paper was supported by the Fund of the Sahmyook University in 2018.
* ㈜씨엠테크 기술사사무소 대표이사, ceo@@cmtes.co.kr
** 건국대학교 정보통신대학원 초빙교수, dskim@kisac.co.kr
*** 교신저자, 삼육대학교 컴퓨터메카트로닉스공학부 교수, hwkim@syu.ac.kr

1. 서론

인터넷, 소셜미디어, IoT 등 개인이 일별 평균 발생시키는 상호작용 횟수가 2015년에는 하루 평균 85건에 불과했는데 2025년에는 하루 평균 4,785건, 거의 8초에 한 번씩 이메일, 센서 등 각종 데이터와의 상호작용이 일어나게 될 것으로 예상된다. 이런 신기술 발전에 따른 데이터 폭증과 더불어 데이터 위변조, 삭제, 탈취, 암호화 같은 공격도 지속적으로 늘어나고 있는데 대표적인 것이 랜섬웨어나 SQL 인젝션 등이다(Segate, 2017).

과학기술정보통신부가 발표한 '2018년 정보보호 실태조사 결과'에 따르면 랜섬웨어 피해를 경험한 기업 비율이 지난 2017년 25.5%에서 지난해 56.3%로 30%p 이상 커졌다. 2016년에는 18.7% 정도였다. 과기정통부는 "최근 신종·변종 랜섬웨어 피해범위가 개인이나 기업의 PC를 넘어 의료·운송·제조 등 다양한 산업 현자응로 확산되고 있다"며 "취약점 관리체계 운영, 이용자 보안의식 제고 등 정보보호 강화가 필요하다"고 강조했다(RanCERT, 2019).

다양한 서비스와 데이터 그리고 산업이 융합되는 미래시대의 도래를 앞두고 있는 시점임에도 불구하고 현재 정보시스템의 운영관리와 감리지침은 기존의 범용적 정보시스템 패턴에 근거해 대응하고 있어 이에 대한 개선이 요구된다. 정해진 시간에 정해진 서비스의 제공이 기업 및 국가의 생존과 연결되고 핵심 요소로 작용하고 있으므로 정보시스템의 서비스 연속성 증대를 위한 운영감리의 개선연구가 필요하며, 본 연구에서는 정보시스템의 비즈니스 연속성이 IT서비스 관리에서 서비스의 전달과 지원 부분에만 초점이 맞추어져 있어 신기술 및 신종 보안요소에 의한 피해를 극복하고 안정성을 높이는데 한계가 있음을 제시하고 이를 탈피하기 위한 ISO 22301에 기반한 정보시스템 감리의 추가적인 점검항목을 제안한다. 비즈니스 연속성의 차원에서 정보시스템 장애로 인한 서비스 중단 때문에 발생하는 업무에 대한 피해를 최소화하고 안정성을 높이기 위해 제공되는 정보시스템 운영감리의 현황에서 발생할 수 있는 문제점을 제시하고 이를 개선하고자 최적화된 방향성과 점검항목을 제안하고자 한다.

2. 관련 연구

2.1 ISO22301 기반 비즈니스 연속성 관리

"2001년 9·11테러로 인한 전 세계적인 혼란, 2011년 태국 홍수로 인한 혼다자동차의 완성차 전량 폐기 등 각종 테러와 자연재해로 인한 위험요인이 증가하면서 이에 대비하는 사회 안전 분야에서의 표준화 요구가 높다. 이에 국제표준화기구는 사업의 중단을 초래할 수 있는 사고가 발생했을 때 조직이 효과적으로 대응하고, 사전에 계획한대로 제품과 서비스 공급을 지속할 수 있도록 필요사항을 규정한 ISO 22301 국제표준을 제정하였다" (ISO/IEC 22301, 2012). 즉 ISO 22301은 조직이 예기치 않은 사고가 발생하더라도 원활하고 안정적으로 비즈니스 연속성을 보장할 수 있어야 한다는 것이다. 그렇지 않을 경우 심각한 경제적 및 법적 부담을 질뿐만 아니라 이미지까지 실추될 수 있다. ISO 22301은 조직이 중단적 사고에 대한 대처, 손실 가능성의 축소, 각종 대응 및 사업의 원상회복을 위해 문서화된 경영시스템을 수립하고, 이 시스템을 실행, 운영, 모니터링 및 지속적인 개선활동을 하기 위한 요구사항을 규정하고 있다(Korean Standards Association, 2018).

ISO 22301은 모든 산업분야 및 활동에 적용할 수 있도록 조직별 다양한 위협에 대한 영향을 파악해 효과적인 대응능력 및 회복능력을 구축하는 프레임워크를 제공 한다. ISO 22301은 PLAN - DO - CHECK - ACTION 의 PDCA 사이클을 통해 지속적으로 개선하는 구성을 가지고 있다(Park, 2017).

Tab. 2-1 PDCA life cycle of ISO 22301[6]

단계	ISO 22301 PDCA 모델 단계별 설명
Plan (계획수립)	조직의 전반적 정책과 목표에 맞는 결과를 산출하기 위해 사업연속성 개선과 관련한 정책, 목표, 통제, 프로세스 같은 절차 수립
Do (구현 및 이행)	사업연속성 정책, 목표, 통제, 프로세스 같은 절차를 실행 및 운영
Check (모니터링 및 검토)	사업연속성 정책과 목표에 대비한 성과의 모니터링과 검토 그리고 검토결과의 경영자 보고, 이에 따른 시정 및 개선에 대한 결정과 권한 부여
Act (유지관리 및 개선)	검토결과에 따라 BCMS 적용범위 개선, 사업연속성 정책과 목표의 재평가, 시정조치를 통한 BCMS 유지관리 개선

2.2 ISO22301의 8대 자원 요구사항

ISO 22301 8.3 사업연속성 전략 요구사항에 따라 기업은 업무영향분석 (Business Impact Analysis)과 위험평가(Risk Analysis) 결과에 근거하여 비즈니스 연속성 확보를 위한 전략적 옵션 실행의 자원 요구사항을 결정해야만 한다. 기업에서 사업연속성 전략 수립 시 고려되는 경영 자원의 종류가 많이 있겠지만 국제표준 에서는 다음의 8가지 자원 유형을 최소 필수 요건 대상으로 정하고 있다(Park, 2017).

가. 인력(People)

나. 정보 및 데이터(Information and Data)

다. 건물, 작업환경 및 관련 유틸리티

라. 시설, 장비 및 소모품(Facilities, equipment and consumables)

마. 정보 및 통신기술시스템

바. 운송수단(Transportation)

사. 재무(Finance)

아. 공급업체/협력업체(Partners and suppliers)

2.3 ISO22301 기반 비즈니스 연속성 관리

ISO22301 기반의 비즈니스 연속성 관리시스템의 구축은 초기 추진주체 및 적용범위의 결정에서 부터 다음의 그림에 나와 있는 순서를 따른다[4].

Fig. 2-1 PDCA-based building process by step[5]

이를 통해 갑작스런 정보시스템의 중단사고에 대비할수 있으며 현재 및 미래의 리스크 식별과 관리 능력의 제고 그리고 조직 구성원의 참여 및 이해도 향상, 비즈니스 중단의 영향과 빈도 감소, 사고 대응 능력의 향상과 복구비용 절감, 사전 연습을 통한 가동중단시간 최소화, 조직 회복력을 입증하여 경쟁력 우위확보, 조직의 명성과 신용도 제고 등이 가능하다. 이 같은 비즈니스 연속성관리의 구축효과의 이해를 돕기 위해 그림을 통해 제시하면 다음과 같다 (ISO/IEC 22301, 2012).

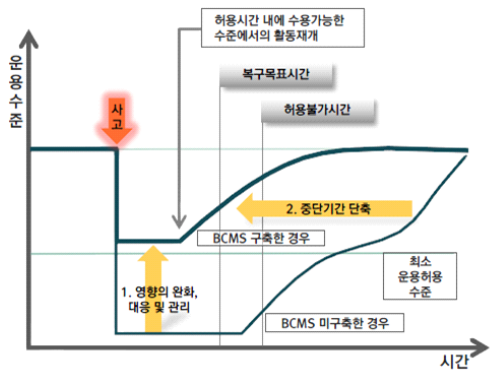

Fig. 2-2 Operating level by time of business continuity management system[1][5].

2.4 정보시스템 감리점검 프레임워크

감리시행시 고려사항에 따라 기본적인 틀을 구성하고 세부지침을 작성하는 출발점의 역할을 수행하는 것이 감리 프레임워크 이다.

“시스템 운영감리는 대부분 위탁운영 용역을 대상으로 실시하고 있으며 자체 운영시에는 내부감리의 형태로 수행된다. 2004~2005년 보급된 ‘정보시스템운영관리지침’ 이 운영관리 분야의 기본적인 지침이 되고 있다” (Korea National Information Society Agency, 2008).

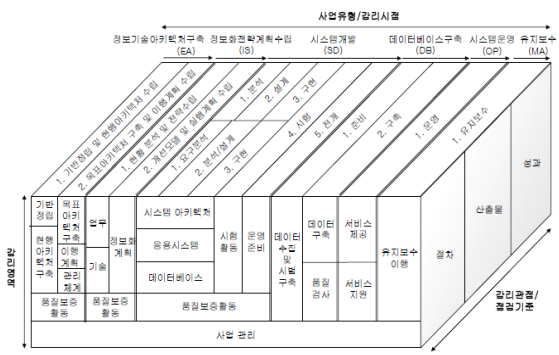

Fig. 2-3 Information systems audit framework[3]

국제적으로는 eSCM, ITIL 등의 ITSM 체계가 제공되어 있으며 ISO20000으로 국제인증 규격화 되어 있다.

감리는 절차, 산출물, 성과의 3가지 관점을 기준으로 점검을 진행하는데 해당 감리관점별 점검기준과 특성은 다음과 같다(Ko, 2012).

Tab. 2-2 Check items criteria of information aystems audit by perspective

감리 관점	점검 기준	관련 특성
절차	계획 적정성	인력운영계획, 사업수행계획 등 관련 계획 수립 적정성
	절차 적정성	개발, 운영, 유지보수의 절차적 적정성 그리고 위험, 일정, 형상, 품질, 인력, 변경관리 절차 등의 적정성
	준수성	계획대비 준수의 적정성 그리고 위험, 품질, 일정, 형상, 인력, 변경관리 등의 절차, 활동준수 적정성
산출물	기능성	기능의 충분성, 정확성, 완전성, 상호 운용성, 연계성
	무결성	데이터 정합성, 무결성 및 정확성
	편의성	사용 편의성, 운영 편의성, 학습성,
	안정성	복구의 신속성, 서비스 연속성, 시스템 안정성,
	보안성	시스템 기밀성, 안정성
	효율성	정보자원 활용의 효율성, 업무 효율성, 시스템 확장성, 기술발정 부합성, 응답시간 신속성
	준거성	산출물 관련기준, 표준, 방법론, 절차 준수성
	일관성	분석성, 추적성, 변경성, 유지보수성, 현행화
성과	충족성	업무, 기술적 요건의 만족, 과업범위 충분성, 성과목표의 달성
	실현성	구체성, 투자대비 효과성, 실현가능성, 성과목표 달성, 시스템 사용가능성

3. 비즈니스 연속성 증대를 위한 운영감리 점검항목

비즈니스 연속성 증대를 위한 정보시스템 운영감리의 점검항목 도출은 한국인터넷진흥원의 시스템 운영 및 유지보수 감리지침과 ISO 22301 표준을 비교하여 제시하였다. 제시한 항목의 근거는 정보시스템의 운영감리 지침과 비즈니스 연속성 재고를 위한 ISO 22301의 요구사항을 비교 분석하여, 연관성을 상, 중, 하로 구분하였고 연관성에 따라서 개선과 신규, 유지 항목으로 정리하여 제시하였다.

3.1 서비스 연속성 관리 부문의 점검항목

기존 정보시스템 운영 및 유지보수 감리지침의 기본 점검항목 중에서 서비스 연속성 관리부문의 감리시 개선할 사항을 아래 표와 같이 도출하였다. 점검항목 내용으로는 “예방점검, 백업/복구, 재해대응 방안 등 서비스 연속성 관리체계를 적정하게 수립하여 관리하고 있는지 여부” 를 검토항목으로 하였다. 기존의 서비스 연속성 관리 분야의 점검항목에 ISO

22301의 요구사항을 근거로 추가 점검항목을 도출하였다.

Tab. 3-1 Audit check items of service continuity management based on ISO 22301

검토항목	산출물 예시
-예방점검 계획수립, -예방점검 실시 및 개선 -모의훈련 -경영진의 서비스 연속성 지원계획	01. 운영정책 및 지침서 02. 서비스수준협약서 03. 예방점검계획서 04. 경영진 지원계획서 05. 지속개선 계획서 06. 조치이행 보고서
-백업 및 복구 정책의 수립 -백업/복구 시행 및 개선 -백업 및 복구 기술의 보유와 인력현황	01. 백업 복구정책 02. 서비스수준정의서 03. 백업신청서 04. 전문기술 지식보유현황서
-재해복구계획 수립 및 준비 -재해대응 훈련 및 개선 -재해복구시스템 위협요소의 대응 및 개선	01. 재해복구계획서 02. 서비스수준정의서 03. 신기술 위협요소 대응방안 계획서 (랜섬웨어 등 감리팁) 04. 지속개선 계획서
-전산센터 기반시설의 구축 -정기 점검 및 유지 보수 -전산 센터 인력과 보유기술(신규)	01. 전산실 설비 점검일지 02. 소방설비 점검표 04. 보유기술, 인력현황서
-조직 특성 고려한 관리체계	01. 조직 특성별 우선순위표 02. 인적구성 전문성 지표 03. 최신기술의 적용 확인서
-최신기술 적용의 정책 수립 -최신기술의 대응 점검체계	01. 최신기술의 적용계획서 02. 최신기술의 점검계획표 03. 최신기술 점검 결과서

3.2 성능, 가용성 관리 부문의 점검항목

기존 정보시스템 운영 및 유지보수 감리지침의 기본 점검항목 중에서 성능 및 가용성 관리부문의 감리 시 개선할 항목을 제시하였다. 점검항목 내용으로는 “성능 및 가용성 관리체계를 적정하게 수립하여 관리하고 있는지 여부”를 검토항목으로 하였다.

Tab. 3-2 Audit check items of performance and availability management based on ISO 22301

검토항목	산출물 예시
- 성능관리 계획 수립 - 성능 측정 및 개선 - 성능 관리 체계에 대한 경영진 지원계획	01. 성능관리 계획서 02. 성능관리 절차서 03. 경영진 지원계획 04. 지속개선 계획서
- 가용성 관리 계획 수립 - 가용성 분석 및 개선 - 가용성 관리체계에 대한 경영진의 지원과 개선 계획 - 신 위협요소의 내부, 외부인력 관리	01. 성능관리 계획서 02. 성능관리 절차서 03. 성능분석 결과보고서 04. 경영진 지원계획 05. 위협요소의 내부 외부 인력 검토서 06. 지속개선 계획서

4. 연구의 검증 및 결과

제 3장에서 제안한 ISO22301기반 비즈니스 연속성 관리를 접목하여 도출한 정보시스템 운영감리 신규 점검항목에 대한 적합성을 검증하기 위해서 구글독스와 이메일 그리고 직접 설문조사 방법을 이용하였다. 설문 응답자의 특성을 파악하고자 업무영역, IT 영역, 운영 및 유지보수 감리경험 그리고 운영관리와 비즈니스 연속성관련 경험을 조사하였고 이를 토대로 운영감리 개선에 대한 적합성여부를 검증하였다.

4.1 개선 점검항목의 설문조사 개요

설문조사의 대상은 다섯 개의 업무군으로 분류해서 진행하였는데 첫 번째는 정보시스템 감리법인 근무 또는 개별 감리원들을 대상으로 하였고, 두 번째는 기획, 사업관리, 품질관리자를 프로젝트관리로 총칭해서 분류 하였다. 세 번째로는 정보시스템의 개발자로 SI부문과 SM부문을 모두 포함시켰고 네 번째는 서버분야, 네트워크분야, DB분야, 보안분야의 정보시스템 운영, 관리자를 대상으로 정했으며 마지막으로 보안담당자와 그외의 IT업무자를 대상으로 하였다.

설문조사는 2018년 10월 27일부터 11월 10일까지 실시하였고 감리원 23명, 프로젝트 관리 13명, 시스템운영 관리자 10명, 개발자 6명, 보안담당자 1명으로 총 53명이 응답하였다.

설문대상의 비즈니스 연속성 관련 업무 경험에 대한 설문은 5년 단위로 분류하여 최대 15년 이상을 기준으로 분류하였고 15년 이상의 경험을 가진 응답자는 없는 것으로 조사됐다.

Tab. 4-5 Survey on key areas of business continuity

구분	서비스수준관리	성능/가용성관리	서비스연속성관리	보안관리	아웃소싱관리	계
인원(명)	3	11	37	2	0	53
분포(%)	5.7	20.8	69.8	3.8	0	100

Tab. 4-1 Results on business continuity-related work experience

구분	5년미만	5년~10년	10년~15년	15년이상	없음	계
인원	24	15	8	0	6	53
분포	45.3	28.3	15.1	0	11.3	100

운영 및 유지보수 감리의 필요성에 대한 설문 결과 대상자의 100%가 필요하다고 응답했다.

Tab. 4-2 Results for the need for operational and maintenance audit

구분	필요하다	필요없다	소계
인원	53	0	53
분포	100	0	100

설문대상의 운영 및 유지보수 감리의 점검항목이 상세화 되어야 한다는 필요성에 대한 설문은 대상자의 98.1%가 필요하다고 응답했다.

Tab. 4-3 Survey on the necessity of detailing the inspection of operational maintenance audit

구분	필요하다	필요없다	소계
인원(명)	52	1	53
분포(%)	98.1	1.9	100

설문대상의 운영감리의 비즈니스 연속성 관련한 점검항목의 상세화가 필요하다는 대상자의 98.1%가 필요하다고 응답했다.

Tab. 4-4 Survey on the necessity of detailing the inspection of business continuity-related audit

구분	필요하다	필요없다	소계
인원(명)	52	1	53
분포(%)	98.1	1.9	100

설문대상의 비즈니스 연속성 증대를 위한 운영감리의 핵심분야에 대한 설문은 기존 항목을 보기로 제공하였으며 서비스연속성이 가장 높은 69.8%로 조사됐다.

4.2 운영감리 개선 점검항목의 적합성 평가

ISO22301기반 운영감리 개선 점검항목에 적합성을 검증하기 위해 각각의 분야별 개선 점검항목에 대한 적합여부를 매우적합(5), 적합(4), 보통(3), 부적합(2), 매우부적합(1)으로 표기하는 5점 리커드 척도를 적용하였다.

제안한 정보시스템의 비즈니스 연속성 증대위한 전체 점검항목의 적합성 평가의 평균은 4.63으로 매우 높은 적합도를 보였으며 표준편차도 0.81로 계산되어 분산의 분포도 넓지 않게 조사되었다.

4.2.1 서비스 연속성 관리의 감리 점검항목

제안한 서비스 연속성 관리분야의 12개 개선 점

검항목의 모두가 평균 4.5 이상의 적합성을 얻어 전반적으로 매우 적합하다는 평가를 받았으며 전체 12개의 제안 점검항목의 평균은 4.71로 성능/가용성관리, 서비스수준관리 측면보다 더 높은 평균적합도를 나타내었다.

Tab. 4-6 Result of conformity survey questionnaire by service continuity management audit check items

검토 항목	세부검토항목	평균	표준 편차
경영진의 서비스 연속성 지원계획	서비스연속성 관리의 경영진 지원계획을 검토한다.	4.71	0.84
	서비스연속성 관리의 경영진 보고와 승인을 받았는지 확인한다.	4.69	0.83
백업/복구 인력과 보유기술	백업 및 복구정책의 수립과 시행 개선을 위한 전문기술의 보유와 인력현황을 확인한다	4.60	0.79
재해복구 시스템의 위협요소에 대한 대응 및 개선	암호화 공격 등 재해복구 시스템의 신기술 위협요소에 대한 대응 방안이 수립되어 있는지 확인한다.	4.58	0.78
	재해복구시스템의 위협요소에 대한 지속적 개선체계를 검토한다.	4.66	0.81
	재해복구시스템 위협요소의 대응을 위한 전문기술의 보유와 인력현황을 확인한다.	4.85	0.91
전산센터 인력과 보유기술	전산 장비에 대한 유지보수 계획을 수행할 인력과 보유기술의 적정성 검토한다.	4.68	0.82
	전산 장비에 대한 유지보수에 대한 경영진의 지원계획을 확인한다.	4.75	0.86
조직 특성 고려한 관리체계	각 조직의 인력구성, 보유기술 현황, 표준절차를 반영한 정보시스템 서비스 연속성 관리 계획을 확인한다.	4.71	0.84
	각 조직 특성을 고려한 서비스 연속성 관리요소별 상세 지침서와 절차서를 확인한다.	4.64	0.80
최신기술 적용의 정책 수립 및 대응 점검체계	주기적으로 신기술 발전에 따른 정보시스템의 서비스 연속성 측면의 영향분석과 대응계획을 확인한다.	4.73	0.85
	신기술 발전에 따른 조직의 정보시스템 서비스 연속성 관리분야의 지속개선 체계을 확인한다.	4.69	0.83

4.2.2 성능/가용성 관리의 감리 점검항목

성능/가용성 관리분야의 5개 개선 점검항목에서도 최저 평균이 4.47로 전반적으로 높은 적합성 점수를 얻어 매우 적합하다는 평가를 받았다.

Tab. 4-7 Result of conformity survey questionnaire by performance/availability audit check items

검토 항목	세부검토항목	평균	표준 편차
성능 관리 체계에 대한 경영진 지원	성능 관리부분의 경영진 지원계획을 검토한다.	4.66	0.81
	성능 관리부분의 개선활용에 경영진의 보고와 승인을 받았는지 확인한다.	4.66	0.81
가용성 관리체계에 대한 경영진의 지원과 개선체계	가용성 관리부분의 경영진 지원계획을 검토한다.	4.51	0.75
	가용성 관리부분의 개선활동에 경영진의 보고와 승인을 받았는지 확인한다.	4.47	0.73
	신기술 적용에 따른 정보시스템 성능/가용성 관리분야의 지속개선 체계를 확인한다.	4.51	0.75

5. 결론 및 논의

정보시스템의 비즈니스 연속성이 기업과 기관 심지어 국가의 이미지 마져도 추락시키는 필수 핵심요소로 대두되면서 반대급부적으로 관련한 위협요소도 더욱더 증가하고 있는 것이 현실이다. 이미 언급한 랜섬웨어와 같은 CaaS(Crime as a Service)시장이 발달하면서 정보시스템의 비즈니스 연속성은 단순 하드웨어나 소프트웨어의 장애를 대비하는 것에 머물

지 않게 되었다. 비즈니스 연속성을 위해 도입한 재해복구 시스템이 랜섬웨어의 암호화 공격에 의해 동시에 서비스 불능상태가 되는 위험도 발생하는 것이 현실인데 이런 신 위협요소를 점검하는 운영감리 체계는 아직 미흡한 것이 사실임을 제시하였다.

본 연구에서는 이와 같은 시대적 현상에 맞추어 정보시스템의 비즈니스 연속성을 증대시키기 위한 운영감리의 개선 방법으로 하드웨어, 소프트웨어, 네트워크, 인프라 측면의 기술적 점검외에도 경영자의 의지, 추진체계, 신기술요소의 점검 프로세스 등과 같은 관리적 요소의 접목을 통해 개선해 보고자 하였다. 국제표준인 ISO22301의 비즈니스 연속성 관리체계를 정보시스템 운영감리에 접목함으로써 새로운 기술과 위협요소에 대응하는 새로운 프레임워크를 제공하고자 하였다.

정보시스템의 비즈니스 연속성이 더 중요해지는 만큼 관련한 운영감리의 필요성도 더 높아질 것으로 판단한다. 본 연구에서 제시한 비즈니스 연속성 개선을 위한 운염감리 점검항목이 향후 해당 부분의 기초자료로 활용될 수 있기를 기대한다.

Reference

[1] ISO/IEC 22301 (2012), Business Continuity Management System Guidance(ISO/IEC 22301:2012 ‘비즈니스연속성경영시스템 가이던스’, ISO).

[2] K.E Ko, J.T Choi, D.S Kim, and H.W Kim(2012), Design of Audit Model in Web-based Information System, Journal of Digital Convergence, 10(9), 123-136(고경이, 최진탁, 김동수. 김희완(2012), ‘웹 기반 정보시스템에서의 감리모형 설계’, 디지털정책연구, 10권 9호, 123-136).

[3] Korea National Information Society Agency(2008), Information System Audit Guideline Manual 3.0(한국정보화진흥원(2008), ‘정보시스템 감리지침 - 시스템운영 및 유지보수 v1.0’).

[4] Korean Standards Association(2018), ISO 22301 Business Continuity Management System PDCA Model(한국표준협회(2018), ‘ISO 22301 비즈니스 연속성경영시스템 PDCA 모델‘).

[5] Korean Standards Association(2008), ISO 22301 Business Continuity Management System Certification Service Guide(한국표준협회(2008), ‘ISO 22301 비즈니스연속성경영시스템 인증서비스 안내’).

[6] Park, Jang Young (2017), “A Study on the Importance of Resources for Business Continuity,” Soongsil University Master’s Thesis (박장영(2017), ‘기업의 사업연속성 확보를 위한 자원 중요도에 대한 연구’, 숭실대학교 석사학위논문).

[7] RanCERT (Ransomware Computer Emergency Response Team Coordination Center) (2019), https://www.rancert.com/bbs/bbs.php?mode=view&id=595&bbs_id=news&page=1&part=&keyword=

[8] Seagate(2017), IDC’s Data Age 2025 study, sponsored by Seagate, April 2017.

Joo, Nak Wan (ceo@cmtes.co.kr)

Joo, Nak Wan is a CEO of Ltd. CMTES. He received the Master degree in the Graduate School of Information Communication at Konkuk University. He has many certificate as a Professional Engineer(P.E.) in Information Systems Management, Chief Information System from Korean Ministry of Science and Technology, PMP, CISSP and CISA. His current research interests include database security/server recovery, information system audit, security and consulting.

Kim, Dong Soo (dskim@kisac.co.kr)

Kim, Dong Soo received the bachelor's degree in the Department of Computer Science from Kwanwoon University in 1981. He received the Ph.D. degree in the Management Information System from Kookmin University in 2005. He has three Certificate as a Professional Engineer(P.E.) in Information Systems Management, Computer Application System, and Computer Communications from Korean Ministry of Science and Technology. He is a chief consultant in the department of Information System Auidt at KISAC company and an invited professor in the Graduate School of Information Communication at Konkuk University. His current research interests include u-city audit, e-business, and information system audit.

Kim, Hee Wan (hwkim@syu.ac.kr)

Kim, Hee Wan is a professor in the Department of Computer Engineering at Shamyook University. He received the Ph.D. degree in the Department of Computer Engineering from Sungkyunkwan University in 2002. He has two Certificate as a Professional Engineer(P.E.) in Information Systems Management and Chief Information System from Korean Ministry of Science and Technology. His current research interests include database, information system audit, database security, software engineering.

Design of Operation Management Check Items of Efficient Information System for Improvement of Business Continuity based on ISO 22301

Nak Wan Joo* · Dong Soo Kim** · Hee Wan Kim***

ABSTRACT

In this paper, we have studied the improvement of operational control for the enhancement of business continuity of information system becoming more important with the development of information technology such as big data, Iot, and artificial intelligence. The operational management and audit guidance of the current information system, which is coming in the fourth industrial age, where various services, data and industries are converged, is based on the existing general information system pattern and needs to be improved. The provision of services at fixed times is linked to the survival of enterprises and countries and serves as a key element. Therefore, it is necessary to study the application of optimized check items of the operation audits to minimize the service interruption damage of the information system and to provide the stable service in terms of business continuity management. To accomplish this, the check items presented in the operational control of the information system were derived by combining the PDCA step contents and 8 resource requirements provided in ISO 22301. From the point of view of increasing the business continuity according to the derivation criteria of the inspection items, the operational inspection check items were derived by exemplifying the improved check items and review items of the information system operation audit and the products to be checked during the operational audit. The check items were divided into management audit improvement check items for service continuity management, and operational audit improvement check items for performance and availability management. The average score of the IT professionals' survey on the suitability of the proposed checklist was 4.63, which was concluded to be appropriate.

Keywords: business continuity, information system operation audit, check items, ISO22301, PDCA

* First Author, CEO of Ltd. CMTES
** Invited Professor, Graduate School of Konkuk University
*** Corresponding Author, Professor, Division of Computer & Mechatronics, Sahmyook University