

기업의 정보보호 영역에서 Six Sigma 추진 과제선정에 관한 연구

남상훈*, 임종인**

*SK Telecom, swnam@sktelecom.com

**고려대학교, jilim@korea.ac.kr

A Study on the Selection of Six Sigma Project theme in Enterprise Information Security Domain

Sangwhun Nam*, Jong-in Lim**

*SKTelecom, Seoul Korea

**CIST, Korea University

요 약

본 연구는 기업이 경영혁신 방침으로 Six Sigma 추진시 정보보호영역에서의 과제선정에 대한 기준을 제시한다. 기업은 윤리경영을 기초로 사업과 서비스를 통한 수익창출을 목적으로 한다. 기업은 안정적인 사업, 서비스의 정보환경을 확보,유지하기 위해 지속적인 보안활동을 통하여 Risk를 줄이는 작업을 해오고 있다. 기업의 정보보호 활동과 패턴은 초기의 정보보호 기본기능을 도입, 구축하는 단계에서 탈피하여, 점진적으로 종합적인 관리체계로 수렴되고 있으며 산출되는 관련 정보와 Data의 정규화를 기초로 정량적으로 관리가 이루어 지는 시점에 와 있다. 그러나, 정보보호 침해사고 예방 및 대응활동, 예측 불허한 상황에서 발생하는 보안사고, 책임문제의 발생, 정성적으로 관리되는 상황 등은 정보보호 영역의 Six Sigma 추진시 과제선정의 어려움으로 작용한다. 정보보호 영역에서 Six Sigma 과제 선정은 일반적인 Six Sigma 과제 선정과는 다르게 정보보호 특성을 고려하여 선정하여 추진하는 것이 바람직하다. 정보보호 활동에 대한 기업의 투자효과도 비재무적 성과외에 경제적 가치요소를 기초로 재무적 성과를 산출하고, 관리하여야 한다. 국내 기업들이 Six Sigma를 경영혁신 기법으로 확대 적용하고 있는 상황에서 정보보호 영역의 Six Sigma 과제선정에 대한 제안을 통하여 정량적 목표수준 관리에 의한 성공적인 Six Sigma 성과를 달성할 수 있도록 함에 있다.

1. 서론

기업의 존재 이유는 윤리적인 경영하에서 수익창출을 통하여 인류사회에 기여함에 있다. 기업은 사업환경의 변화와 다양한 Risk의 증가에 대한 전략을 수립하여 대응, 발전해 오고 있다. 특히 정보보호에서의 Risk 관리는 움직이는 표적을 관리하는 것과 같이 동적이면서, 정량적인 관리가 요구된다. 기업의 경영혁신 기법의 하나인 Six Sigma와 정보보호 활동도 이의 일환으로 이해된다. 기업의 정보보호 활동과 패턴은 이제 정보보호 기본기능을 도입, 구축하는 초기에서 탈피하여, 점차적으로 관리 체계안으로 수렴되고 있으며 산출되는 정보보호관련 정보와 Data의 정규화를 기초로 정량적으로 관리되는 시점에 와 있다.[1]

그러나, 정보보호 침해사고 예방 및 대응활동, 예측 불허한 상황에서 발생하는 보안사고, 책임문제의 발생, 정성적으로 관리되는 상황 등은 정보보호 영역의 Six Sigma 추진시 과제선정의 어려움으로 작용한다. 정보보호 환경의 변화와 기업이 Six Sigma를 추진하는 배경에 대해 기술하고, SixSigma의 성공요인과 그 성공요인의 주된 사항인 과제선정에 대한 중요성에 기초하여 과제선정 요인 및 접근방법에 대해 정의한 후과제선정시 정보보호 특성과 선정방법론에 따른 선정 고려요소를 통해 기준을 제시하고자 한다. 이를 통해 국내 기업들이 Six Sigma를 경영혁신 기법으로 확대 적용하고 있는 상황에서 정보보호 영역에서의 Six Sigma 과제선정에 대한 제안을 통해 성공적인 Six Sigma 성과를 달성할 수 있도록 함에 있다.

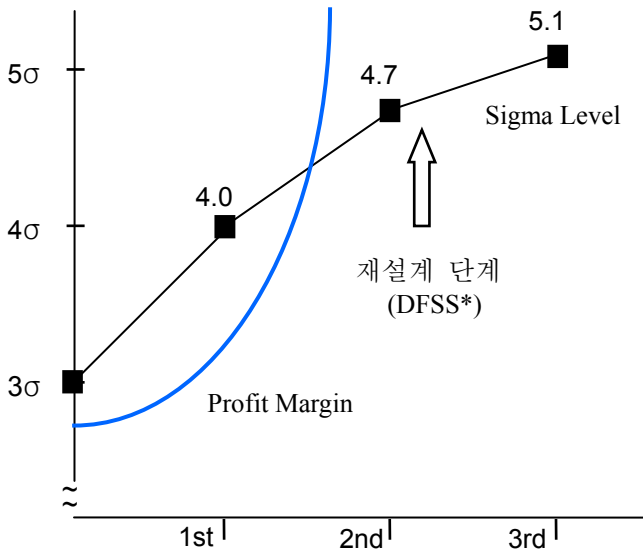
2. 기업의 정보보호 & Six Sigma

2.1 기업 정보보호 환경의 변화

기업의 경영과 사업환경의 변화는 기업에게 기회와 위기의 상황을 동시에 만들어 내고 있다. 2003 년말 2,920 만명이 인터넷을 사용하던 상황에서 2004 년말 140 여만명이 증가하여 3,000 만명을 돌파하였다. 더구나 그중 1,190 여만명이 초고속 인터넷을 사용하고 있는 상황이다. 기업은 유비쿼터스 사회로 진입되고, 기술이 융,복합화되는 상황에서 심각한 해킹, 워/바이러스 유포, 네트워크 불법침입, 불건전 정보유통 및 개인정보유출 등과 같은 정보화의 역기능에 대응해야 한다. 기업의 정보보호 활동도 종합적인 정책과 상위 사업연속성 관련체계와 연계하며 진화하고있다. [2]

2.2 기업에서 Six Sigma 도입배경

기업은 총체적 고객만족 경영전략으로 또하나의 미래 환경에 대비한 차별화된 경쟁우위 확보를 위해 Six Sigma 를 추진하고 있다. 그러나 핵심적인 도입배경은 Six Sigma 라는 과학적 접근 방법과 체계적 개선 방법론을 토대로 프로세스 산포를 줄여, 고객 만족도를 제고하고 비용을 절감하여 기업의 수익을 향상하는데 있다. 1996 년 GE 가 도입 적용하여 2000 년까지의 5 년간 총비용 \$2.1B 에서 총효과 \$5.4B, 순이익 \$3.3B 를 얻는 성과를 보였으며, 우리는 2002 년 는 6 시그마 경영을 도입한 13 개 대기업이 총 3 조원 이상의 비용을 절감한 것으로 추정(한국경제 2002.4.30)되고, POSCO 는 2006 년 기업가치 35 조원을 예상한다.



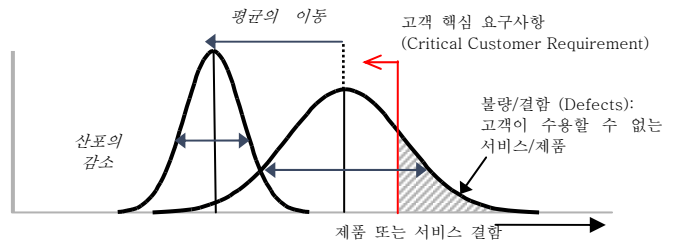
*DFSS (Design For Six Sigma)

(그림 1) Six Sigma 수준과 이윤폭 [3]

2.3 Six Sigma 개념과 추진방법

경영성과의 평균 수준을 높일 뿐만 아니라 산포를 줄임으로써 제품 및 서비스의 결과가 완벽하게 ‘고객 요구’에 부응하도록 하여 문제를 해결하고자 한다.

(그림 2) Six Sigma 개념



<표 2> Six Sigma 추진방법

핵심 품질요소 (CTQ*) 파악	고객입장에서 기업의 경영활동 재조명
핵심 프로세스 도출	CTQ 를 좌우하는 프로세스와 결함을 발생시키는 부분을 집중탐색
프로세스 측정, 분석,개선,통제	결함원인을 찾고, 개선활동으로 원인을 제거한 뒤 지속적으로 통제

*CTQ (Critical to Quality)

2.4 Six Sigma 의 특징

Six Sigma 는 통계 데이터에 근거한 철저한 분석, 고객만족에 초점, 재무성과로 연결, Six Sigma 전문인력에 의해 주도, 기본적으로 Top Down 식의 전개를 기본으로 하고 있다.

<표 3> Six Sigma 특징

검증된 개선 방법론 활용	DMAIC* 방법론과 DFSS 방법론에 따라 최적화된 해결 방안 도출
Fact-Based Management 추구	과학적 접근법 및 Tool 을 이용한 통계적/실험적 검증 수행
지속적인 Process Control	개선된 프로세스의 성과 추적 및 성과 수준의 지속적 관리

*DMAIC (Define, Measure, Analyze, Improve, Control)

3. Six Sigma 체계와 과제선정

3.1 Six Sigma 의 성공요소

기업은 다음과 같은 성공요소에 기초하여 기업상황과 특성을 고려, 전략과 대책을 수립 추진하여야 한다.

<표 4> Six Sigma 추진 성공요소 - 6R

Right Leadership	정확한 현실인식에 바탕을 둔 Top 의 강력한 의지와 리더십의 구현
Right Road-Map	Six Sigma 의 장기비전, 전략, 목표 일정계획 등의 합리적인 작성, 운영
Right People	해당영역의 개선필요성과 Six Sigma 의 기법을 인지하고 Top 의 방침을 펼칠 수 있는 우수한 인재의 활용
Right System	경영혁신을 지원하는 목표지향적인 시스템의 가동 및 활용 -교육/훈련, 프로젝트운영, 성과평가, 경영정보, 고객품질 시스템 등
Right Project	회사의 주요성과지표(KPI*)와 고객의 요구사항(VOC**)에 기초하여 CTQ 를 반영한 적절한 프로젝트의 선정
Right Culture	Six Sigma 의 활동을 일상업무 일환으로 받아들이는 기업문화의 조성

* KPI (Key Performance Indicator), **VOC (Voice of Customer)

3.2 Six Sigma 과제선정의 중요성

Six Sigma의 과제선정은 Six Sigma의 성공요소의 하나다. 그러므로 성공적인 과제의 선정은 곧 Six Sigma의 바람직한 추진에 근간이 되며, 어느 조직이든 과제의 선정기준과 선정작업은 주요 Issue 사항이다. Six Sigma의 가장 중요한 출발점은 바로 과제의 선정이라 할 수 있다. 기업이 수익달성을 위해서 수립하는 경영전략과 목표에 연계하여 과제를 선정하고 과제는 전사적인 목표와 추진방향을 갖게 된다. 제대로 선정된 과제는 기업과 조직이 원하는 목표달성을 가능하게 하면, 이를 통해 달성된 목표는 경영층과 조직구성원이 수용하는 결과로서 관리되고 평가된다.

3.3 Six Sigma 과제 선정요인

기업은 Six Sigma 과제 선정시 사전 해당과제와 관련된 전제사항을 크게 고객의 요구, 기업의 요구 그리고 현장의 요구사항을 정확히 파악하고 있어야 한다. [4]

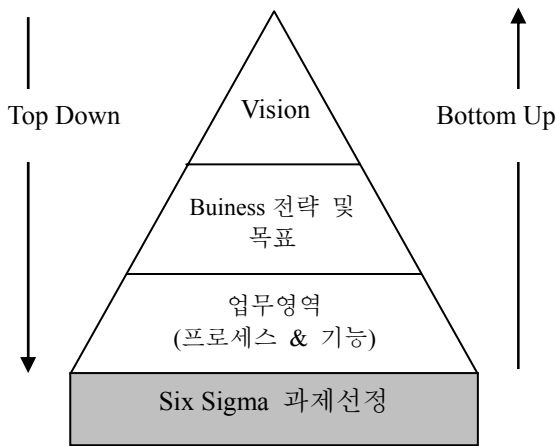
<표 5> Six Sigma 과제선정 요인

고객의 요구	고객 CTQ 파악과 고객과의 대화, 시장조사, 품질기능전개(QFD/ Quality Function Deployment)에 의한 파악
기업의 전략	전사차원의 전략은 부서별 또는 사업장별로 전개되며 SWOT 분석과 목표
현장의 요구	프로세스 단계의 문제점 파악 및 개선활동 과정의 CTQ 파악을 위해서는 SIPOC 을 통해 명확히 정의하고 고객을 위한 가치 창출이라는 프로젝트의 최종목표를 정의

* SIPOC (Supplier, Input, Process, Output, Customer)

3.4 Six Sigma 과제선정 방법

과제선정 유형은 Top-Down 접근법과 Bottom-up 접근법과 이의 Sandwich(절충형) 접근법으로 구분된다.



(그림 3) Six Sigma 과제선정의 접근 [5]

과제선정은 현장의 실무적인 입장에서 Sandwich(절충형 방식)으로 접근하는 것이 바람직하다.

<표 6> Six Sigma 과제선정 방법

Top-Down 접근법	기업의 주요 사업 목적을 고려한 후에 그와 관련된 Champion(임원)이 선정하여 성과지표와 목표를 설정하는 방식
Bottom-Up 접근법	일선관리자와 실무진들에 의해 과제의 성과지표, 목표를 수립하고 이를 기초로 협의하여 선정
Sandwich (절충형) 접근법	Top-Down 접근법과 Bottom-Up 접근법을 조합, 병행한 형태로 일선관리자와 실무진들에 선정과제(안)이 제시되고, 임원이 성과지표, 목표에 기초하여 선정

4. 정보보호 영역에서 Six Sigma 과제선정

4.1 정보보호 특성의 고려

정보보호 영역의 Six Sigma 추진시, 정보보호 특성인 기밀성, 무결성, 가용성의 특성을 가지고 있어 과제 선정시 이를 반영하여야 한다. 정보보호의 특성은 고객의 요구사항을 수렴하되 고객의 불만사항등 현장의 부정적인 시각에 대한 기업의 Vision 과 발전을 위한 전략이 우선하여 반영되는 것이 일반적이다. 정량적 분석과 접근을 기초로 하는 Six Sigma 에 있어서 산출되는 정보와 Data 의 분석은 정보보호의 현상과 문제점을 객관화 할 수 있는 기준과 지표등을 통해 논리수용력을 가지고 있어야 한다. 이를 위해, 정보보호전문요원과 현업의 긴밀한 협의를 통해 정량화되어지는 결과의 타당성검증이 필요하다.

4.2 정보보호 영역에서 과제선정

과제선정 방법론의 하나인 BAP(Business Alignment Planning)는 전략과 연계하는 방법론으로 기업의 전략을 확인하는 것으로 시작하여 필요한 경우엔 각 전략을 달성하기 위한 Six Sigma 비전을 설정하기도 한다.

<표 7> BAP 추진 Road Map

구분	1 단계	2 단계	3 단계	4 단계
전략적 BAP	전략연계	프로세스 연계	고객연계	중점추진 영역도출
운영적 BAP	잠재실행 과제도출	실행과제 확정	BB 선정	경영진 승인

4.2.1 전략적 BAP

1) 전략연계 단계

성과향상에 영향이 큰 기업이 KPI 및 핵심 추진전략을 확인하는 단계로서 정보보호 영역은 대부분의 기업은 System 및 신규 사업,서비스의 안정성 조기 확보차원에서 중요한 전략적 KPI 를 정의하고 있다. 정보보호를 기업의 사업,서비스 추진시 핵심전략 및 경쟁우위요소로 활용하고 있는나를 판단, 연계한다.

2) 프로세스연계 단계

전략 목표 달성과 가장 연관성이 높은 핵심 프로세스 선정하는 단계로 전략적 목표로 정의된 사업,서비스관련 프로세스에 정보보호의 Cross 지원기능을 정의하고 활용한다.

3) 고객연계 단계

핵심 프로세스에 대한 고객의 요구 및 기대사항 파악하는 단계로 고객은 고객정보와 대고객서비스에서 안정성을 고려한 인증, 정보수집, 관리를 원하고있다. 보호기능에 대한 고객의 부정적 반응도 염두에 둔다.

4) 중점 추진영역 도출단계

고객의 핵심 요구 사항을 고려하여 큰 그림인 전략적인 그림(Big Y)를 도출하는 단계로, 주안점은 정보보호 영역은 고객의 핵심 요구사항보다 기업의 전략적인 접근이 우선하며 주요 사업,서비스에 대한 지원기능,성과에 대한 지표관리와 정량화 작업이 필요하다.

4.2.2 운영적 BAP

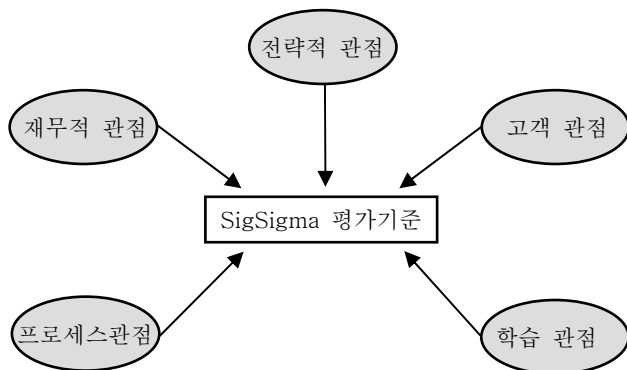
1) 잠재실행 과제도출

중점 추진영역과 연계된 상세 프로세스의 이슈로부터 실행과제를 도출하는 단계로 정보보호 영역에선 정보보호 관리 및 정책적인 부분, System 및 Network 과 OA 등의 정보보호 기술부분, 관리와 기술부분에 공통으로 지원되는 부문을 다루게 된다. 기업에서의 중요도, 시급도의 순서로 잠재실행 과제를 정의한다.

2) 실행과제 확정

실행과제의 과제 적합성 평가를 통한 실행과제 확정하는 단계로 구성원간 논란이 가장 많이 발생한다. 기업이 정보보호 영역에서 산출되는 정규적인 Data 를 관리하는 수준이면 이슈(침해사고 및 보안투자 등)에 대한 우선순위를 고려하여 관리영역안으로 수렴하는 것이 필요하다. 그리고 수렴되는 정보보호의 정규화된 Data 를 기초로, 객관적인 평가, 통계적인 관리기능 강화를 통해 정보보호 정책 및 투자결정에 지원, 활용되어야 한다. [6] Six Sigma 의 정량적 관리기법을 통해 정보보호의 문제점을 기업의 관리체계안으로 흡수, 수렴하는 것이 중요하기 때문이다. 과제의 확정은 평가를 통해 선정하게 되는데 기존의 재무적관점, 고객관점, 프로세스관점, 학습관점외에 정보보호요소를 반영한 전략적 관점을 적용하여야 한다. 평가는 객관적인 평가를 위해 BSC(Balanced ScoreCard) 를 활용하는 것이 좋다.

(그림 4) Six Sigma 과제선정 평가관점



평가관점의 내용은 다음과 같다.

<표 8> Six Sigma 과제선정 평가내용

전략적 관점	기업생존과 발전을 위한 사전 Risk 의 제거, 최소화 및 사업, 서비스의 경쟁우위요소로 활용
재무적 관점	매출,이익의 증대, 비용절감 요소
고객 관점	고객만족도, 시장점유율 향상
프로세스관점	프로세스효율 향상 및 리드타임 감소
학습 관점	지식자산의 증대 및 업무능력의 향상

3) BB 선정

실행과제를 수행할 전문인력 선정 및 과제 기술서 작성단계로 직,간접적으로 관여해온 정보보호전문요원을 활용하는 것이 필요하며, 점차적으로 정보보호 기능과 연계되는 관련 조직의 요원으로 확대, 선정해 간다.

4) 경영진 승인

과제와 수행인력에 대한 경영진의 승인 및 확인단계이다.

4. 결론

기업이 경영혁신 방침으로 Six Sigma 를 선택, 추진시 올바른 과제의 선정은 주요 성공요인중의 하나이다. 정보보호 영역에서 과제를 선정하게 될 경우 다음과 같은 정보보호의 특성을 고려하는 것이 바람직 하다.

- 1) 정보보호의 과제선정은 기업에서 예상되는 Risk 를 제거 또는 최소화하는 전략적 관점에서 추진하고 경쟁 우위요소로 활용할 수 있도록 하는 것이 필요하다.
- 2) 전략적 목표로 정의된 사업,서비스관련 프로세스에 정보보호의 Cross 지원 기능을 정의하고 활용한다.
- 3) 정보보호에서 중점 추진과제의 도출은 가능하며, 정보보호영역은 고객의 핵심 요구사항보다 기업의 전략적 접근이 우선하며 주요 사업, 서비스에 대한 지원기능,성과에 대한 지표관리와 정량화 작업이 필요하다.
- 4) 정보보호에 대한 경영층의 인식과 정보보호 프로세스가 정립 정도를 고려한 기업의 수준에 따라 정보보호의 기밀성, 무결성, 가용성의 비중에 따라 잠재실행 과제를 도출한다.
- 5) 기업이 정보보호 영역에서 산출되는 정규적인 Data 를 관리하는 수준이면, 이슈에 대한 우선순위를 고려과제로 선정, Six Sigma 의 정량적 관리기법을 통해 정보보호의 문제점을 기업의 관리체계안으로 흡수, 수렴하는 것이 필요하며, 객관적 평가를 위해 BSC 를 활용하는 것이 바람직하다.

참고문헌

[1] 신일순(2004) “정보보호경제학적 의미에 대한소고”
 [2] 남상훈(2005) “TSM Function Model based on COSO Framework (TIEMS-ICIS 2005)”
 [3] Mikel Harry(1995) “A Breathrough Strategy by Profitability”
 [4] 서철호(2000) “6 시그마 Proj.테마 선정에 관한연구”
 [5] 박성현,이명주,정목용(2005) “6 시그마 혁신전략”
 [6] 남상훈(2005) “기업의 사업연속성을 고려한 통합보안 관리기능에 관한연구”, 제 23 회 KIPS 춘계학술발표대회 논문집(12-1)