IBM Global Technology Services

Thought Leadership 백서

2012년 7월

IT와 전략적 비즈니스 목표의 연계

비즈니스에 대한 IT 리스크의 능동적 관리 방식

IBM

목차

개요

오늘날 사실상 모든 기업에서 정보 기술(IT)은 핵심적이고 필수 불가결한 구성 요소입니다. 이와 같은 IT 활용은 분명한 장점을 제공하지만 그와 동시에 중대한 비즈니스 과제를 부여합니다. IT의 복잡성 및 수많은 비즈니스 영역과의 상관성 때문에 각 기업은 내재된 리스크에 과거 어느 때보다도 취약한 상태가 되었습니다. IT에 영향을 주는 사건은, 예전에는 IT 부서 차원에서 해결할 수 있었지만, 지금은 비즈니스의 전반에 파장을 미칠 수도 있습니다. 데이터 유실, 파손, 접근 차단, 보안 사고, 인프라 장애 등은 순식간에 일반 대중에게까지 알려져 기업의 생산성, 평판 그리고 전략적 목표 달성 능력에 심각한 타격을 입히곤 합니다.

IT 위협 요인이 비즈니스 전반에 광범위한 영향을 미칠 수 있음에도 불구하고, 대부분의 기업에서 IT 리스크 관리 계획과 전략적 비즈니스 이니셔티브의 연계를 고려하지 않고 오히려 전통적인 리스크 관리 방식을 고수하는 편입니다.

이 기존의 방식은 불확실한 세상에서 일어날 불상사에 대해 비용에 기초한 분석을 실시하고, 제대로 문서화될 수 없는 변수로부터 얻어진 지표를 구현하는 데 중점을 둡니다. 이는 신뢰도가 낮은 방식이며, IT 리스크 파악 및 관리에 도움이 되지 않을 수도 있습니다.

전 세계의 IT 및 정보 시스템 전문가들이 회원으로 참여하는 비영리 단체인 ISACA에서는 IT 리스크를 "기업에서 IT의 사용, 소유, 운영, 관여, 영향 및 도입과 관련하여 일어나는 비즈니스 리스크"라고 정의합니다.[1]

IT 리스크가 비즈니스에 미칠 영향을 더 효과적으로 관리하는 방법은 통합적인 관점에서 접근하는 것입니다. 그러면 IT 서비스 제공 기능이 비즈니스 목표 및 목적 달성을 위해 안정성, 유연성과 민첩성을 향상시키는 데 필요한 바와 더 직접적으로 연계될 수 있습니다. 따라서 현재의 IT 서비스 제공 상태가 비즈니스 목표에 가져올 리스크를 더 정확하고 시기적절하게 파악하고, 우선 순위에 기초하여 올바른 리스크 완화 조치를 취할 수 있습니다.

이 백서에서는 IT에 의존함으로써 발생할 수 있는 비즈니스 과제와 리스크를 살펴보고 기존의 IT 리스크 관리 방식이 더 이상 적합하지 않은 이유를 조명합니다. 그리고 리스크 관리를 종합적인 전략적 비즈니스 이니셔티브와 연계하는 체계적인 방식을 소개합니다. IT 팀은 IT와 비즈니스 요구사항을 더 긴밀하게 연계함으로써

해당 기업이 더 경제적으로 운영되고 정보에 기초한 사려 깊은 의사 결정을 통해 더 효과적으로 변화에 대처하도록 뒷받침할 수 있습니다.

날로 진화하는 비즈니스 과제 - IT 리스크 관리

정보 기술의 진화가 시작된 초창기에 IT는 단순히 기업의 정보를 처리하고 안전하게 데이터를 저장했다가 백업하는 기능을 제공했던 하드웨어와 네트워크를 의미했습니다. 시간이 흐르면서 비즈니스 효율성을 높일 필요성이 제기되고 주요 비즈니스 트랜잭션의 실행에서 기술에 대한 의존도가 높아지고 더 많은 정보와 더 복잡한 분석 리포팅이 요구되면서 IT는 기업 자체의 경영과도 밀접하게 연관되면서 비즈니스 성공에 중요한 역할을 맡게 되었습니다. IT에서 비즈니스 목표를 지원하는 범위는 더욱 확대되어 날로 증가하는 데이터와 애플리케이션을 수용하고 효용 가치가 있도록 체계화하고 접근 가능한 방식으로 저장하는 일도 포함되었습니다. 뿐만 아니라 IT 경영진은 회사에서 기대하는 결과를 내놓기 위해 다양한 프로세스, 인재, 설비와 전략을 도입하는 책임도 맡고 있습니다. 더 줄어든 IT 예산과 인력으로 이러한 책임을 이행할 뿐 아니라 더욱 까다로워지는 유연성 및 무중단 가용성에 대한 요구도 해결해야 합니다.

이와 같이 IT에 대한 의존도가 높아지면서 IT 리스크가 비즈니스 전반에 미치는 영향력도 증가했습니다. 비즈니스 재해복구(business resilience)가 우선시되고 리스크 관리가 비즈니스 부서와 프로세스까지 포함하도록 확대되고 표준화된 것은 이러한 리스크를 줄이는 데 분명 도움이 되었습니다. 그러나 상당수의 비즈니스 리더들은 여전히

자신이 이끄는 조직에서 효과적으로 IT 리스크를 파악하고 관리할 수 있는가에 의구심을 갖고 있습니다. IBM이 실시한 세 가지 연구 조사의 결과도 이러한 현실을 반영합니다.

- 리스크 관리 및 컴플라이언스에 대한 우려를 나타낸 CIO (chief information officer): **58%**[2]
- 회사의 전반적인 IT 리스크 완화 방식이 "평균 수준"이거나 "부실"하다고 평가한 CIO: **34%**[3]
- 리스크 관리 기능을 공식적으로 갖추지 않았다고 밝힌 고위 임원: **30%**[4]

기존의 IT 리스크 관리 방식

IT 리스크 관리에 대한 불신이 그토록 커진 이유는 무엇입니까? 취약점이 광범위하게 악용될 때 IT 서비스에 대한 위협 요인은 비즈니스에 대한 리스크로 작용합니다. 아직도 상당수의 기업이 IT 서비스 제공의 경제적 영향에 초점을 맞추는 매우 협소한 시각으로 리스크를 분석하고 있습니다. 이러한 "전통적인" 접근법은 화재, 홍수, 정전, 기물 파손, 테러 공격, 보안 장애와 같은 전형적인 위협 요인을 파악하는 것으로 시작하며 이러한 위협이 비즈니스 가용성, 복구 가능성과 보안에 미칠 잠재적 영향을 기준으로 삼습니다. 하지만 전형적인 범주에 속하지 않은 위협 요인은 간과하기 쉽습니다. 어떤 기업에서 위협 요인을 파악하거나 그 가능성을 정확하게 판단하지 못하면 실제로 그러한 위협에 얼마나 취약한지 평가할 수 없습니다.

전통적인 방식에서는 일반적인 위협 요인을 파악한 다음 잠재적 비즈니스 비용, 손실 운영상의 영향에 따라 이 위협 요인의 해결 우선순위를

결정합니다. 이러한 변수를 정량화하고 정성화함으로써 리스크 분석에 유용한 정보를 얻을 수 있겠지만 의사 결정 우선 순위를 비즈니스 목표와 연계하길 원하는 경영진의 요구사항을 해결하지는 못합니다. 이는 전통적인 접근법의 심각한 한계이며, 리스크 관리를 컴플라이언스 위주의 기능으로 보지 않고 리스크에 기초한 의사 결정을 위한 전략적 분야로 강조하는 ISO (International Organization for Standardization)'s (ISO) 31000 표준에도 부합하지 않습니다. 이 기존의 방식에서는 기업의 목표 및 전략적 비즈니스 이니셔티브와의 연결 고리가 없으므로 이러한 목표를 달성하는 데 리스크가 어떤 영향을 미치는지 입증할 수 없습니다.

어떤 기업에서 위협 요인을 파악하거나 그 가능성을 정확하게 판단하지 못하면 실제로 그러한 위협에 얼마나 취약한지 평가할 수 없습니다.

통합적인 관점의 접근

기업에서 IT 사용에 따른 비즈니스 리스크를 제대로 파악하려면 기존의 표준에 한정되지 않고 IT와 비즈니스의 전략적 방향을 연계하는 더 광범위한 시각으로 IT 리스크를 조명해야 합니다. 특히 다음과 같은 이점을 제공하는 접근법이 필요합니다.

- **IT와 비즈니스 요구사항의 긴밀한 연계 –** 정보에 기초한 사려 깊은 의사 결정을 통해 더 신속하게 변화에 대처함으로써 비즈니스 민첩성을 확대할 수 있습니다.
- **브랜드와 수익성 보호** – IT 인프라에 대한 위협 요인, 비즈니스에 미칠 잠재적 영향 또는 이점, 해당 기업의 리스크 허용 수준을 평가함으로써 현실적인 전략을 수립할 수 있습니다.
- **전략적 비즈니스 이니셔티브 실현을 위한 IT 서비스 수준 개선** – 더 정확하고 적합한 정보를 제공하여 IT 리스크 관리를 지원합니다.
- **기업의 재정 및 평판에 미칠 악영향 최소화** – 부정적 보도, 경제적 손실, 벌금이나 기타 처벌로부터 기업을 보호합니다.
- **경쟁 우위 강화** – 경쟁사가 미처 파악하지 못한 리스크에 대해서도 사전 계획에 따라 대처할 수 있습니다.

각 기업은 일반적인 리스크 관련 기법을 전략적 비즈니스 이니셔티브와 직접적으로 연계함으로써 주요 성과 지표(key performance indicator, KPI)와 주요 리스크 지표(key risk indicator, KRI)를 더 수월하게 문서화하고 전략적 목표에 미칠 영향 또는 기여도에 따라 리스크의 우선 순위를 결정할 수 있습니다. 또한 균형 잡힌 리스크 관리 계획을 이행하고 명확한 커뮤니케이션 계획을 수립하고 지속적으로 리스크 지표를 모니터링할 수 있게 됩니다.

더 강력한 지표의 중요성

점점 더 많은 기업에서 전략적 비즈니스 이니셔티브의 구현과 달성에 관여하는 모든 레벨의 경영진이 KPI를 성과 추적 및 관리의 지표로 삼고 있습니다. 경영진에게 회사의 지난 실적과 전략적 비즈니스 이니셔티브의 향후 전망을 개괄적으로 전달하는 보고서에 KPI를 취합하여 수록합니다. 지표는 리스크를 추적하고 관리하는 데에도 필요합니다. 그러나 KPI는 과거의 성과 데이터를 기반으로 하므로 이 용도로는 적합하지 않습니다.

그보다는 KRI를 초기 경보 지표로 삼아야 합니다. 즉 새로운 리스크가 실제로 발생하기 전에 알림으로써 해당 기업이 목표를 달성할 기회를 포착하거나 만일의 부정적 영향을 최소화할 수 있습니다. 이 지표는 기업이 리스크에 대처하고 적절한 대응 조치를 취하기에 충분한 시간을 확보할 수 있을 만큼 일찍 작동해야 합니다.

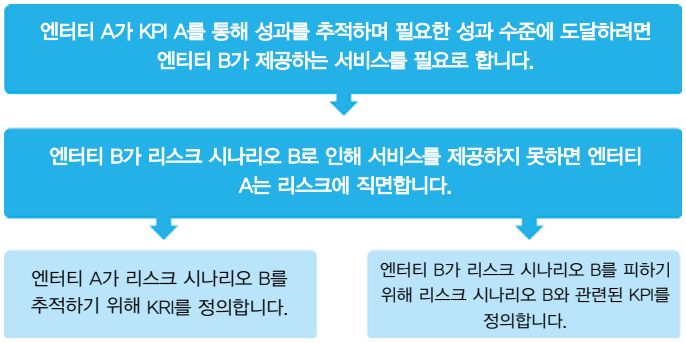
KPI와 KRI가 서로 다른 지표이지만 서로 관련 있습니다. KPI는 비즈니스 성과를 추적하는 데 쓰입니다. KRI는 기업에게 임박한 변화에 대해 경고하는 데 쓰입니다. 비즈니스 엔터티는 서비스의 측면에서 상호 의존 관계에 있으므로, 공급자가 서비스를 제공하지 못하면 여기에 의존하는 수요자는 리스크에 직면합니다. 이러한 "기능(capability)" 리스크 때문에 수요자가 성과 목표를 달성하지 못할 수도 있으므로 KRI를 통한 관리가 필요합니다.

예를 들어 설명하자면,

고객과의 정보 교환을 위해 새로운 채널을 개설하는 것이 바람직한 고객 서비스를 제공하는 데 필수적이고 "고객 중심 주의"를 지향하는 더 광범위한 전략적 이니셔티브 실천의 일환이라면, 다음과 같은 몇 가지 비즈니스 KPI를 적용할 수 있습니다.

- 새로운 시장 기회에 더 신속하게 대처하고 더 일찍 ROI를 실현할 수 있도록 규 채널의 구현 시간을 (가급적 3개월로) 단축
- 새로운 채널을 통한 신규 고객 유치율 향상
- 매일 예정된 가동 시간 연장(가급적 하루 24시간 체제로)

이 신규 채널이 스마트폰에서 액세스할 수 있는 새로운 인터넷 웹 사이트를 기반으로 한다면 IT에 대한 의존도는 확실하며, 따라서 해당 기업은 IT가 기대했던 서비스 기준을 제공하지 못하면 이를 잠재적 리스크로 간주할 수 있습니다. (회사에서는 3개월 또는 그 미만으로 기대하는) 채널 구현 시간은 (현재 IT 팀에서 6개월로 추정하는) 새로운 인터넷 웹 사이트의 설계, 개발 및 구현에 필요한 시간으로부터 직접적인 영향을 받을 수 있습니다.



KPI: 주요 성과 지표(key performance indicator)
KRI: 주요 리스크 지표(key risk indicator)

그림 1: KPI 및 KRI 지표의 모니터링은 전략적 비즈니스 이니셔티브의 관리에 도움이 됩니다.

IT의 다음 단계는 개선이 필요한 부분을 찾기 위한 격차 분석, 새로운 IT 서비스 구현에 그토록 긴 시간이 소요되는 이유를 규명하기 위한 근본 원인 분석을 수행하는 것입니다. 이를테면 근본 원인 분석에서 a) 애플리케이션 개발에 매우 긴 시간이 걸리는 이유는 개발 시스템의 가용성 부족 때문이고 b) 새로운 애플리케이션을 위한 신규 하드웨어 도입이 늦어지는 이유는 복잡한 구매 절차 때문이라는 결과가 나왔다면, 적시에 새로운 서비스에 대처하기 위한 IT 서비스의 "민첩성" 요인에 대한 선행 지표가 되는 2개의 KRI가 확보된 셈입니다.

비즈니스 요구사항의 변화에 따라 알맞은 신규 또는 변경된 IT 서비스를 제공하는 대처 능력의 측면에서 IT 역량의 격차가 있음이 분명합니다. 따라서 이 회사는 전략적 목표를 달성하지 못할 위험이 있습니다. 이러한 리스크를 모니터링하려면 현업 팀에서 구체적인 KRI를 정의하고 IT 팀에서는 "신규 서비스 구현에 필요한 시간" 영역의 개선을 추적할 KPI를 정의해야 합니다.

IT Risk Spectrum

IBM은 더 체계적이고 통합적인 접근법의 필요성에 부응하여 IT Risk Spectrum™ 을 개발했습니다. 이는 각종 IT 리스크를 5개의 논리적 범주로 통합한 것입니다. 이 리스크 범주를 통해 현재의 IT 서비스 제공 상태 및 리스크 완화 우선 순위가 비즈니스 목표에 미칠 영향을 판단할 수 있습니다. 기업의 비즈니스 요구사항과 IT를 더 긴밀하게 연계하고 따라서 IT를 통해 비즈니스 민첩성을 향상시키는 데 IT Risk Spectrum을 활용할 수 있습니다. 그림 2에서 보여 주는 것처럼, 그림 2에서 IT Risk Spectrum은 5개의 IT 리스크 범주로 구성되며, 이 범주는 구체적인 비즈니스 목표, 즉 민첩성과 적합성, 확장성과 성능, 보안과 데이터 보호, 정확성과 적시성, 가용성과 복구 가능성에 연결 지을 수 있습니다.

민첩성과 적합성: IT 서비스는 목표한 비즈니스 성과를 거두기 위해 빠르고 효과적이고 경제적인 방식으로 적응하고 혁신할 수 있어야 합니다.

확장성과 성능: IT 팀은 변화하는 비즈니스 요구사항에 따라 IT 용량과 성능을 변경함으로써 그러한 변화에 대처할 수 있어야 합니다. 뿐만 아니라 모든 서비스와 구성 요소를 대상으로 애플리케이션/데이터 성능과 처리 속도 지표를 추적할 수 있어야 합니다. 비즈니스 사용자와 고객의 성능 및 용량 요구사항에 부합하도록 스스로 조정하는 기능도 필요합니다.

보안과 데이터 보호: 시스템 관리, 아카이빙, 공식적인 리포팅 및 조사 기능을 활용하여 높은 수준의 보안을 유지할 수 있습니다. 제대로 데이터를 보호하기 위해서는 인프라 및 물리적 보안도 필요합니다.

정확성과 적시성: 비즈니스 및 운영 프로세스의 전반에서 정확하고 시기적절한 정보 흐름을 유지하는 것은 비즈니스 성과에 매우 중요합니다. 데이터 소스(내부 또는 외부)를 비롯한 데이터 품질이 구체적인 기준에 부합해야 비즈니스 목표를 뒷받침할 수 있습니다.

IT Risk Spectrum	실제 리스크 사례
민첩성과 적합성: 목표한 비즈니스 성과를 거두기 위해 더 빠르고 효과적이고 경제적인 방식으로 적응하고 끊임없이 혁신합니다.	고객에 대한 다양한 유지 관리 요구사항을 해결하지 못해 어려움을 겪던 한 유럽 은행은 IT 서비스의 범위를 확대하여 새로운 내부 고객도 수용할 수 있도록 멀티 플랫폼 성과 관리 솔루션을 도입했습니다. 그 결과, 서비스 민첩성과 유연성이 향상되었고 내부 고객 만족도가 상승했으며 관리 비용이 줄어들었습니다.
확장성과 성능: 비즈니스 요구사항에 더 부합하는 성능 수준을 유지하고 비즈니스 서비스 볼륨의 변화를 적절히 수용합니다.	한 미국 소매업체는 온라인 쇼핑몰 이용자 수가 전례 없이 급증하여 쇼핑몰의 기능이 마비되는 사태에 이르렀습니다. 수요에 따른 확장이 불가능하여 판매 기회를 잃고 이미지가 실추되었으며 온라인 구매 고객의 신뢰도 떨어졌습니다.
보안과 데이터 보호: 알맞은 액세스 제어를 제공하고 기업의 정보와 자원을 보호할 수 있도록 지원합니다.	도쿄의 한 제조사는 방화벽과 안티바이러스 소프트웨어를 업그레이드하지 못했습니다. 해커가 침투하여 고객 데이터에 접근했고 이는 계약 취소와 고객 신뢰도 하락으로 이어졌습니다.
정확성과 적시성: 알맞은 사용자에게 적합한 시점에 정확한 데이터를 전달하여 정보에 기초한 더 현명한 의사 결정을 내릴 수 있게 합니다.	한 유럽 은행에서 애플리케이션 업데이트를 적용했다가 고객 데이터가 손상되었고 시스템 장애가 며칠간 이어졌습니다. 계정 업데이트 지연 시간이 허용 한도를 넘어섰고 미디어에 널리 보도되면서 수사의 필요성까지 제기되었습니다.
가용성과 복구 가능성: 중단 없이 시스템을 운영하고, 필요에 따라 비즈니스 기대 수준에 부합하도록 장애로부터 복구합니다.	터키의 한 통신사에서 전례 없이 많은 비가 내리는 바람에 데이터 센터가 침수되는 일이 발생했습니다. 문서화하고 검증된 복구 또는 연속성 전략이 없었기 때문에 고객 서비스가 중단되었고 이 업체는 처리 시간 손실, 계약 취소, 브랜드 이미지 실추를 감수해야 했습니다.

그림 2: IT Risk Spectrum은 비즈니스 목표에 기초한 5가지 범주로 구성됩니다.

가용성과 복구 가능성: 비즈니스 및 IT 담당 임원은 이 비즈니스 요구사항을 해결할 수 있도록 반복 가능하고 충실한 프로세스를 적용하고 적절한 지출을 진행하는 방식으로 가용성 및 복구 전략을 함께 수립해야 합니다. 회사는 각종 사건, 문제와 장애에 시기적절하게 대처할 수 있도록 앞선 방법론과 도구를 사용하고 지속적인 개선 프로세스도 마련해야 합니다.

IT 리스크는 기업의 핵심 비즈니스에 끊임없이 부담으로 작용합니다. IT Risk Spectrum는 규범적인 관점에서 기업을 조명하고 IT 리스크가 구체적인 비즈니스 목표에 미칠 영향을 분석하므로, 이러한 리스크가 핵심 비즈니스에 어느 정도 영향을 미칠지 판단하는 데 도움이 됩니다.

또한 핵심 비즈니스의 주요 구성 요소를 검토하여 IT Risk Spectrum과의 연관성을 확인하고 이를 제대로 모니터링할 수단을 찾아야 합니다. IBM은 그러한 구성 요소를 검토 가능한 상태로 만들고 의존 관계 분석 및 병렬 분석을 모두 실시할 수 있도록 기업을 "분해"하기 위해 Core Business Framework를 적용합니다. 이 프레임워크는 6개 도메인으로 구성되어 기업 경영에 필요한 모든 (내부 및 외부) 구성 요소를 다룹니다.

- **사람.** 회사를 구성하는, 역할과 책임이 부여된 인적 자원 및 교육과 커뮤니케이션을 통해 기술력을 유지하는 데 필요한 프로세스
- **프로세스.** 기업이 개방적인 프로세스 프레임워크에서 비즈니스 프로세스 모델링을 통해 핵심 비즈니스를 수행하고 IT 전략과 거버넌스, 비즈니스 연속성, 백업과 복구, 서비스 관리 등을 통해 기술 환경을 유지하는 방식
- **기술.** 서버, 스토리지 시스템, 네트워크, 데이터베이스, 애플리케이션, 텔레포니 등 기업의 비즈니스 프로세스를 지원하는 장비와 도구
- **공급자.** 기업의 경영 및 비즈니스 활동에 필요한 중요 자료, 서비스와 정보를 제공하는 업체와 정부 기관
- **인프라스트럭처.** 기업에서 제어하는 구성 요소로서 물리적 보안, 전기 시스템, 수도, 냉각 등의 기능 지원
- **"엑소스트럭처(Exostructure)".** 기업에서 제어할 수 없는 에코시스템의 중요 구성 요소로서 전기 공급, 수도 공급, 도로, 운송, 식품 공급, 통신, 거버넌스 등

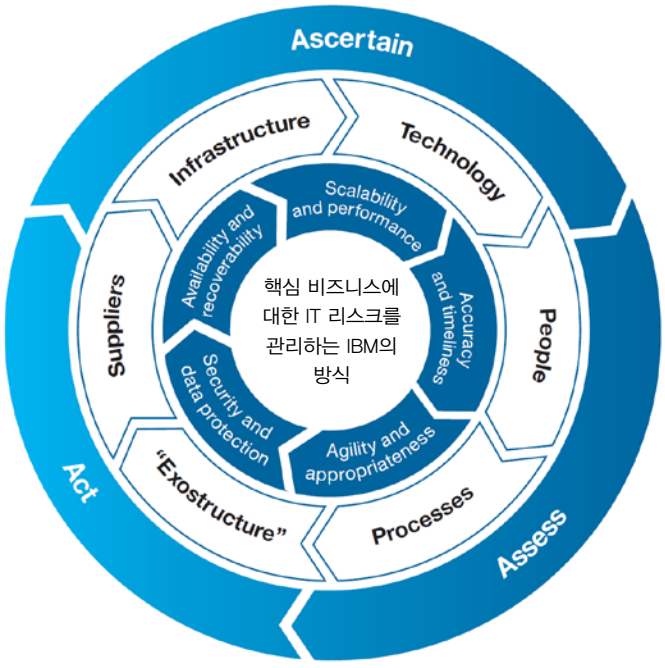


그림 3: IBM의 IT 리스크 관리 방식은 비즈니스와 그 운영 구성 요소에 대한 IT 리스크에 중점을 둡니다.

비즈니스에 대한 IT 리스크를 관리하는 IBM의 방식

IBM은 ISO 31000을 토대로 통합적이고 간결한 리스크 관리 방법을 개발했으며, 이를 IT 영역에 적용한다면 더 우수한 컴플라이언스를 제공하는 리스크 아키텍처를 통해 사실상 ***어떤*** 전사적 리스크 관리 프로그램과도 원활하게 연계할 수 있습니다. 이 방법은 확인(ascertain), 평가(assess), 실행(act)의 3단계로 구성됩니다.

확인

IBM의 IT 리스크 관리 방식의 첫 단계는 IT 리스크 관리 프로그램의 범위와 목표를 정하는 것입니다. 어떤 IT 리스크 프로그램이든 위협 요인과 그 상대적 비즈니스 리스크를 지속적으로 파악, 평가하고 대처하기 위한 활동을 포함해야 합니다. 목표를 확인하고 역할과 책임을 명확하게 정의하지 않으면 이후의 관리 프로세스에서 난관에 봉착합니다. 프로그램 설정 프로세스의 초기 단계에 범위와 역할을 모두 정한다면 새롭게 확인된 IT 리스크의 책임자로부터 이 프로세스와 향후 리스크 완화 조치 요청에 대한 지지를 확보하는 데 도움이 됩니다.

전략적 비즈니스 이니셔티브를 결정하고 IT 리스크 관리 목표를 정의하고 사내외 압박 요인을 판별함으로써 범위를 설정할 수 있습니다. 처음에는 집중적인 내용으로, 향후에는 전사적 영역을 포함하게끔 확장하는 방향으로 프로그램의 범위를 설계합니다. 활동에 필요한 시간, 포함시킬 장소 등도 범위를 결정하는 데 변수로 작용할 수 있습니다. 또한 이 단계에서는 리스크 평가 방법이 선택되고 향후 IT 리스크 관리 프로세스에 대한 평가 시스템의 윤곽이 결정됩니다.

그리고 회사 전체에서 필요한 모든 이해 관계자가 포함될 수 있도록 명확한 역할과 책임을 정의합니다. 다양한 부서의 관계자를 광범위하게 리스크 관리에 참여시키는 것이 현재 전 세계적인 추세입니다.[5] 이와 같이 역할을 정의하면 기업의 IT 리스크 관리 책임을 정하는 데 도움이 되며, 전사적 범위에서 구체적인 역할의 담당자 이름을 제시할 수 있습니다.

평가

비즈니스 목표가 설정되면 전략적 비즈니스 이니셔티브와 관련하여 IT 리스크 영역이 정의됩니다. 이를 위해 IT 서비스와 이 서비스가 지원하는 비즈니스 목표를 직접적으로 연결합니다. 비즈니스 재해복구를 위한 통합적 리스크 관리의 핵심 요소 중 하나는 기업이 직면한 위협 및 기회 요인을 종합적으로 조명할 수 있도록 균형 잡힌 시각으로 다양한 리스크를 평가하는 능력입니다.[6] IT Risk Spectrum과 같은 길잡이를 이용하고 전사적 범위에서 비즈니스 이니셔티브 지원에 필요한 IT 서비스를 분석한다면, 기업이 더 민첩하게 변화에 대처하기 위해 가장 필요로 하는 IT 서비스 영역을 더 수월하게 찾을 수 있습니다. 이러한 이니셔티브를 지원하는 IT 서비스의 관계를 명확하게 이해하는 것도 리스크 평가의 중요한 측면 중 하나입니다.

"오늘날에는 IT 없이 아무 것도 할 수 없는 만큼 IT는 리스크 관리에서 큰 부분을 차지합니다."라고 KS Energy Services Limited의 CEO인 Kris Wiluan은 밝힙니다.[7]

다음 단계는 평가 가능한 IT 리스크를 파악하고 성과 지표를 정의하기 위해 IT 서비스의 "모든 기능"에 대한 분석을 실시하는 것입니다. 그러면 의미 있는 KPI 및 KRI를 확보하고 IT 성과 기능에 기초하여 비즈니스에 대한 IT 리스크를 정량화할 수 있습니다. 이러한 지식을 통해 균형적인 처리 옵션을 정의하여 우선 순위를 정하고, 자신 있게 리스크 완화 솔루션 구현을 위한 로드맵으로 작성하며, 성공에 불리하게 작용할 만한 변화를 모니터링하기 위한 제어 수단을 찾아낼 수 있습니다.

이러한 평가에는 IT 리스크가 현실화되어 제공되는 IT 서비스의 수준이 기대에 미치지 못할 경우 전략적 비즈니스 목표에 미칠 영향도 포함해야 합니다. 이러한 영향 분석은 정량적 평가(직접적인 비용 손실 또는 서비스 수행 비용 증가) 또는 정성적 평가(평판 리스크에 미칠 영향) 모두 가능합니다. IBM ORQ(Operational Risk Quantification) 방식은 다양한 리스크 이벤트의 범주를 분석할 수 있습니다. 여기에는 프로세스 관련 세부 사항을 생략하고 경제적 손실을 기준으로 그 심각도를 직접 측정하는 "하향식(top–down) 이벤트", 프로세스–자원 네트워크를 통해 전파되어 궁극적으로 재정적 영향의 결과를 표시하는 "상향식(bottom–up) 이벤트"가 포함됩니다.[8]

재해복구에 대한 관점을 확대하더라도 전문성 또는 컴플라이언스 리스크를 도외시해서는 안 됩니다. 그보다는 회사 전반의 이해 관계자에 의한 폭넓은 평가가 가능하도록 평가 및 우선 순위 결정 프로세스에 더 다양한 리스크를 포함시킴으로써 재해복구를 향한 발전적인 여정이 되어야 합니다. 평가 단계에서는 KPI 및 KRI 형태의 충실한 성과 및 리스크 지표를 제공합니다. 이러한 지표를 통해 전략적 비즈니스 목표와 이를 뒷받침하는 IT 서비스에 대한 더 우수한 가시성을 확보할 수 있습니다. 리스크 관리 계획을 마련함으로써 파악된 리스크에 대해 제어 또는 보호의 형태로 책임 있고 적절하게 대응하는 등 확실한 결과를 얻을 수 있습니다.

실행

KPI 및 KRI가 문서화되고 비즈니스 전략 목표에 따라 우선 순위가 부여되었다면 균형 잡힌 처리 계획을 이행하고 명확한 커뮤니케이션 계획을 적용하고 지속적으로 리스크 지표를 모니터링할 차례입니다. 이 단계에서는 전사적 범위에서 실행의 책임을 가질 다양한 자원을 배정함으로써 리스크 관리 계획을 이행합니다. 리스크 책임자는 비즈니스 목표와 연계하고 최고 경영진, 현업 부서, IT 전문가, 이사회, 일반 직원까지 포괄하는 회사 전반의 모든 단계에서 더 적극적인 참여를 이끌어낼 수 있도록 IT 리스크를 설정하고 관리합니다.[9]

평가 단계에서 고안된 의미 있는 지표에 따라 지속적으로 IT 리스크를 모니터링함으로써 회사 전반에 작용하는 압박 요인에 책임 있게 대처할 준비를 갖출 수 있습니다. 비즈니스 목표가 변화하더라도 이 동일한 지표를 중단 없이 검토하여 지속적으로 연계해야 합니다. 모니터링에는 리스크 평가 및 KPI 정의의 결과에 따라 IT와 비즈니스의 다양한 영역이 포함될 수 있습니다. 이를테면 "일정대로 또는 조기에 완료된 애플리케이션 개발 및 유지 관리 프로젝트의 비율", "사건 해결까지 경과한 평균 시간" 등이 있습니다.

평가 결과에 따라, 리스크가 현실화될 경우 비즈니스에 미칠 영향을 반영하여 리스크 완화 조치의 선택을 조정해야 합니다. KRI 각각이 모니터링 비용 항목에 해당되므로 모니터링 프로세스를 설정하는 데 많은 비용이 들 수 있습니다. 기업이 더 성공적으로 리스크를 관리하면서 재정적 책임도 다하기 위해서는 최적의 투자 지점을 찾아내는 것이 중요합니다.

기업이 이 새로운 관리 시스템으로 전환함에 따라 확인 단계에서 언급한 대로 고위 경영진의 확고하고 지속적인 지원이 필요하고 또한 내실 있는 커뮤니케이션, 인식 및 교육 프로그램 개발을 위한 알맞은 자원이 필요하게 됩니다. 이러한 프로그램은 더 광범위한 거버넌스, 리스크 및 컴플라이언스 활동에 IT 리스크 관리를 통합하는 데 필요합니다.[10]

뿐만 아니라 모든 이해 관계자가 IT 리스크 프로그램을 인식, 이해하고 활용할 능력을 갖춘다면, IT 리스크 관리가 모든 사람의 직무라는 사실을 효과적으로 강조할 수 있습니다. 이러한 전환 단계에서 모든 레벨의 임직원을 대상으로 교육 및 인식 프로그램을 실시하고, 이해 관계자가 각자의 역할을 이해하고 프로그램에 관련된 여러 단계에 정기적으로 보고할 수 있도록 지원해야 합니다.

요약

전략적 비즈니스 목표를 실현하는 데 필수적인 IT 서비스가 늘어나면서 특별한 리스크와 기회가 생겨나고 있습니다. 과거 어느 때보다도 IT는 안정성, 예측 가능성, 가용성과 강력한 보안을 토대로 주요 비즈니스 프로세스와 핵심 이니셔티브를 지원해야 합니다. IT 사용과 관련된 비즈니스 측면의 리스크를 이해하기 위해서는 회사 전반의 IT 리스크와 IT 서비스에 대한 폭넓은 시각이 필요합니다. IT 서비스 제공에 영향을 주는 물리적이고 자연적인 위협 요인에만 주목하는 기존의 방식으로는 이러한 문제를 제대로 다룰 수 없습니다. 이 글에서 입증한 것처럼, 이제는 IT 팀이 위협 요인에 기초한 영향 평가의 토대를 마련하고 다루는 리스크의 스펙트럼을 넓혀 더 확실하게 기업을 보호하고 전략적 목표 달성을 지원해야 합니다.

통합적이고 체계적인 접근법을 구현함으로써 회사 전반에 자원을 배정하고 의미 있는 지표를 통해 지속적으로 IT 리스크를 모니터링하고 IT 리스크 관리 프로그램을 모든 이해 관계자에게 전달할 수 있습니다. 그러한 능동적인 리스크 관리 문화에서는 더 신속하고 적절하게 대처하고 IT 리스크와 리스크 완화 비용의 사이에서 최적의 균형점을 찾는 것이 가능해집니다.

IBM을 선택하는 이유

IBM은 더 능동적으로 운영 리스크와 그에 따른 비즈니스 중단 문제를 파악, 이해, 관리하고 대처하려는 고객을 위해 IT 리스크 관리 서비스를 제공합니다. IBM과 함께 중단 없이 비즈니스 환경을 운영하면서 더 효과적으로 브랜드를 보호하고 수익성 있는 성장을 지원하며 고객과 파트너 모두로부터 변함없이 신뢰 받을 수 있습니다. IBM 재해복구 전문가가 ISO, ISACA와 같은 산업 표준을 적용하면서 귀사의 환경을 이해하고 고유한 요구사항에 부합하는 맞춤형 재해복구 프레임워크의 구축을 지원하며 평가에 쓰일 자료를 검토하고 문제 해결 및 개선을 위한 로드맵을 마련합니다. IBM은 세계적인 IT 솔루션의 선두 주자로서 다양한 제품과 서비스를 제공하며, IBM 컨설턴트는 이를 효과적으로 적용하여 날로 까다로워지는 리스크 관리의 요구사항을 해결합니다.

추가 정보

IBM Resiliency Consulting Services, IBM의 리스크 관리 방식 또는 IT Risk Spectrum에 대한 자세한 내용은 IBM 마케팅 담당자 또는 IBM 비즈니스 파트너에게 문의하거나 다음 웹 사이트를 참조하십시오. ibm.com/services/continuity

또한, IBM Global Financing은 가장 비용 효과적이며 전략적인 방법으로 여러분의 비즈니스 요구사항에 부응하는 IT 솔루션을 확보할 수 있도록 돕고 있습니다. 신용 자격이 있는 고객들과 협력하여 귀사의 비즈니스 목표에 부합하는 IT Financing 솔루션을 맞춤화하고, 효과적으로 현금을 관리하며, 총소유비용을 향상시켜줍니다. IBM Global Financing은 중요한 IT 투자 및 귀사의 향후 비즈니스 추진을 위한 현명한 선택입니다. 보다 자세한 정보는 www.ibm.com/financing에서 확인하실 수 있습니다.

1 ISACA, www.isaca.org, retrieved June 4, 2012.

2 "The essential CIO insights from the global chief information officer study," IBM, May 2011.

3 "The evolving role of IT managers and CIOs: Findings from the 2010 IBM global IT risk study," IBM, September 2010.

4 "Key trends driving global business resilience and risk: Findings from the 2011 IBM global business resilience and risk study," September 2011.

5 "Key trends driving global business resilience and risk: Findings from the 2011 IBM global business resilience and risk study," September 2011.

6 "Key trends driving global business resilience and risk: Findings from the 2011 IBM global business resilience and risk study," September 2011.

7 "Key trends driving global business resilience and risk: Findings from the 2011 IBM global business resilience and risk study," September 2011.

8 "Operational risk analytics in the context of information technology (IT) infrastructure," IBM, March 2012.

9 "Key trends driving global business resilience and risk: Findings from the 2011 IBM global business resilience and risk study," September 2011.

10 "Operational risk analytics in the context of information technology (IT) infrastructure," IBM, March 2012.

IBM Corporation
IBM Global Services
Route 100
Somers, NY 10589

Produced in the United States of America
July 2012