MARKET SIGNALS™

백 서

적절한 하이브리드 IT 모델을 결정할 때 고려해야 하는 3대 요소

Rimini Street®

요약

하이브리드 IT 모델이 새로운 기준으로 자리잡으면서 공급업체, 고객, 파트너사들이 클라우드를 사용하는 방식과 기업이 취하는 통합과 보안을 향한 접근법이 기업들의 하이브리드 IT 비전에 영향을 미칠 것입니다. 이에 클라우드로 이관할 IT 구성요소를 결정할 시 이 세 가지 요소를 평가해야 합니다.

분석

하이브리드 IT 환경은 기업들이 IT 구성요소 중 일부는 클라우드로 이관하고 일부는 비(非)클라우드 환경에 남겨두고자 실행하는 전략의 결과물입니다("하이브리드 IT를 통한 디지털 혁신 지원" 참고). 기술의 클라우드 이관을 도모하는 대다수 기업은 적절한 속도의 비즈니스 중심 일정에 따라 움직여야만 합니다.

대부분 기업들에게는 모든 애플리케이션을 클라우드로 이관하는 것이 비즈니스상 최선의 선택은 아닐 것입니다. 가령 ERP 같이 촘촘하게 연동된 핵심 시스템을 SaaS로 이관하는 것은 비즈니스 개선에 거의 도움이 되지 않습니다. 한편 대(對)고객 시스템 및 기타 참여 시스템은 SaaS로 구현되면 경쟁 우위를 이끌어낼 수 있습니다. 이렇게 클라우드와 비(非)클라우드의 조합으로 하이브리드 IT 환경이 조성됩니다. 또는 클라우드 전략 실행에 시간이 많이 필요해서 수년 동안 하이브리드 IT 포트폴리오를 유지하는 경우도 있습니다.

IT 관점에서 보면 특히 기존 소프트웨어 라이선스에서 얻는 가치가 더 큰 경우라면 애플리케이션과 그 지원 인프라를 클라우드로 이관하는 것은 최선이 아닐 수 있습니다. 이에 많은 CIO가 인프라만 클라우드로 이관하고 라이선스로 사용하는 애플리케이션은 IaaS에서 운영하는 방식을 선택하고 있습니다. 하이브리드 IT 환경의 또 다른 예시라고 할 수 있습니다.

고려 요소	각 요소가 하이브리드 IT 모델에 미치는 영향
1 다른 IT 생태계와의 상응	하이브리드 IT 모델 구조는 기업이 상호작용하는 생태계들을 포용해야합니다.
2 통합 관련 리스크 수용도	기업의 통합 관련 리스크 수용도는 클라우드를 통해 제공할 수 있는 데이터와 프로세스의 양, 그리고 하이브리드 IT 포트폴리오로 흡수할 수 있는 클라우드 제공업체의 수를 결정하는데 영향을 미칩니다.
3 하이브리드 IT 환경 보안	하이브리드 IT 환경의 안전성과 보안성에 대한 신뢰 수준은 특히 클라우드 공급업체의 보안성을 분명하게 파악하기 힘든 경우 무엇을 클라우드에 구현할지 결정하는 데 영향을 미칩니다.

고려 요소 1: 다른 IT 생태계와의 상응

기업이 상호작용하는 외부 시스템들은 클라우드와 비(非)클라우드 아울러 다양한 모델로 구현됩니다. 기업의 공급업체, 파트너사, 고객들과 유사한 구현 선택지를 택하면 단순화를 통해 비즈니스 가치를 증대할 수 있습니다.

외부적인 관점에서 보면, 기업의 기술 생태계와 상호작용하는 공급업체, 파트너사, 고객의 시스템 위치(클라우드 또는 비클라우드)는 애플리케이션을 SaaS로서 클라우드로 이관하거나 비클라우드에 유지하는 두 가지 경우에서 각각 얻을 수 있는 비즈니스 가치에 영향을 미칩니다. 일례로 의료 산업의 경우 개인정보 보호 규정으로 인해 클라우드 기반 시스템을 업계 전반에서 공유하기 힘들기 때문에 클라우드 이관의 핵심 비즈니스 동인이 이러한 시스템에는 크게 의미가 없습니다.

통합하기 어려운 옵션이나 공급망 간 프로세스를 한층 복잡하게 만드는 옵션을 선택하면 비즈니스 결과를 방해하거나 저하시킬 수 있습니다. 가령 모두가 시스템을 클라우드로 이관한다면 여러분 시스템도 클라우드 이관을 고려하세요. 만약 아무도 이관을 추진하지 않는다면 해당 시스템은 아직 클라우드 이관이 시기상조일 수 있습니다.

내부적으로 보면, IT 조직의 자체적인 시스템 개발 또는 패키지 솔루션 구매 수준이 하이브리드 모델을 구성할 SaaS 솔루션과 자체 개발 솔루션의 비율에 영향을 미칩니다. 또한, 클라우드 개발에 사용하는 도구, 플랫폼, 제품도 하이브리드 IT 모델에 영향을 미칩니다. 상반되는 두 예시를 소개합니다.

> A사는 시스템 개발을 약간 시도해 보지만 SaaS 구성요소를 두고는 구체적인 제품 방향성(마이크로소프트 등)을 설정했습니다. 시스템 개발에도 공급업체의 클라우드 플랫폼을 사용할 가능성이 높았습니다(이 경우 MS Azure). 이렇게 하면 호환성 이슈를 완화하고 제품군 전반에 걸친 공통성에서 더 많은 가치를 이끌어낼 수 있을 것입니다.
>
> B사는 애플리케이션 개발(자사만의 고유한 대(對)고객 뱅킹 솔루션 등)이 주를 이루는 비즈니스 모델을 적용 중입니다. B사의 하이브리드 IT 모델은 사내 개발 전략과 도구 세트를 지원할 수 있는 클라우드 공급업체(AWS 등)를 중심으로 구체화될 것입니다.

클라우드는 빠른 속도로 복잡해질 수 있고 이로 인해 유지보수 및 포트폴리오의 개선이 어려워질 수 있습니다. 즉, 클라우드를 둘러싼 미흡한 의사 결정은 비즈니스의 혁신 및 성장 능력을 저해할 수 있습니다. 호환과 지원이 가능한 기술 포트폴리오를 수립하기 위해서는 클라우드 이관 대상 결정을 둘러싼 철저하면서도 반복 가능하고 일관성 있는 전략이 필요합니다. SaaS는 물론 플랫폼과 도구까지 모두 아우르는 분명한 전략을 세우면 비즈니스를 뒷받침하면서도 유지 및 개선이 용이한 애플리케이션 포트폴리오를 확보할 수 있을 것입니다.

권장 사항:

- **프레임워크 및 애플리케이션 의사 결정 나무를 수립해** 클라우드 이관에 대한 대비 상태를 평가하고 클라우드 방향성을 유기적으로 설정하세요. 목표는 경영진과 IT 조직이 플랫폼 선택, 클라우드 범위, 사용 도구를 둘러싼 방향과 선택지, 영향을 이해하도록 하는 것입니다. 그림 1에서 프레임워크 예시를 확인하세요.
- **비즈니스에 미치는 영향의 심각도**, 리프트 앤 시프트(lift and shift) 같은 작업 수행의 난이도, 다음 현장 하드웨어 또는 OS 업그레이드의 시기와 비용, 애플리케이션의 안정성, IT 인력 확보 능력, 시스템의 수명 장기화 계획(유지 및 교체 기간 특정) 등 전략적 요소를 평가하세요.
- **수치 평가 알고리즘을 만들어** 그 결과를 활용해 우선순위 기반 투자 및 프로젝트 리스트를 작성하세요.
- **이관 전략을 수립하고** 자사 애플리케이션 개발 계획에 부합하도록 업계에 적합한 시계(time horizon)를 설정한 후, 해당 일정을 발표하세요.

클라우드 대비 수준 및 방향성 평가를 위한 프레임워크 예시

비즈니스	**비즈니스 근거**	ABC사는 클라우드 협업 플랫폼으로의 이관에 필요한 실질적이고 가시적인 리더십 겸 후원 조직을 보유함. 비즈니스 및 IT 리더가 전환을 준비 중임.
	비즈니스 사례	TCO 추정치가 나오면 본 영역을 마무리하고 비즈니스 근거를 확정할 수 있음.
인재	**경영진 후원**	ABC사는 중요한 경영진 리더십을 식별함. 프로그램 관리를 위해 공식적으로 클라우드COE(Center of Excellence)을 구성해야 함.
	협업	IT 조직은 경영진과 좋은 관계를 유지하고 있으며 주기적으로 비즈니스 검토를 실행 중. IT 조직은 조직 내 자체적으로, 그리고 경영진과 함께 공식적으로 변경 관리 과정을 이끄는 중.
	변경 관리	최고경영진에게 더 많은 클라우드 도입 유도를 위해 클라우드와 관련해 주기적인 논의 및 발표를 시작할 것을 제안.
거버넌스	**성과 측정**	ABC사는 공식적인 비즈니스 사례를 활용하고 있으며 클라우드 COE 수립을 이끌고 거버넌스 및 컴플라이언스 우려사항을 해소하는 데 클라우드 평가를 활용할 수 있게 될 것임.
플랫폼	**클라우드 제공자**	ABC사는 기존 이용 중인 클라우드 플랫폼이 없음. ABC사는 애플리케이션 클라우드 파트너사를 결정해야 함.
운영	**인프라**	ABC사는 클라우드와의 네트워크 연결성을 증축해야 함. ERP 애플리케이션은 클라우드로 이관될 준비가 됨.
	민첩한 프레임워크	팀에서는 클라우드 제공에서 최상의 가치를 이끌어내는 데 중요한 민첩한 개발(Agile development)을 잘 알고 있음. IT 팀은 선택한 클라우드 제공자로부터 받는 교육을 활용해야 함. 서브스크립션 계약에 포함할 수 있음.
	운영 및 책임 조정	ABC사는 운영 개시 이후 최초 클라우드 구현을 유지보수할 파트너사 활용을 고려하면서 외부 유지보수와 자체 유지보수 간 TCO를 비교해봐야 함. ABC사는 파트너사를 활용함으로써 클라우드 변경 관리 모범 사례를 수립하고 클라우드 내 사업 연속성 계획의 진정한 가치를 온전히 실현할 수 있음.
	협업	
보안	**운영상 클라우드 보안**	ABC사는 모든 환경에 대해 견고한 보안 정책을 보유하고 있음. 조직의 실질적인 강점임.
	문서화된 보안 정책	이러한 정책들을 클라우드용으로 전환하여 적용해야 함. 선택한 클라우드 제공업체로부터 추가 보안 교육을 받을 수 있음.
데이터 통합	**통합 역량**	ABC사는 전사 차원의 통합 관련 팀이 없음. 통합 역량 센터와 클라우드 통합, 관련 프로세스, 정책, 책임 등이 필요함.
	통합 관련 리스크 수용도	ABC사는 데이터 관리 팀이 운영 중이며 클라우드 구현에 적합하지 않은 민감한 데이터와 프로세스를 식별함.
내·외부 IT 생태계	**파트너사 클라우드 전략**	ABC사는 자사의 공급업체, 파트너사, 고객들이 어떤 구성요소를 클라우드로 옮기는지 파악하고 이들과 발을 맞추기 위해 클라우드 프로젝트의 우선순위를 설정함. IT 조직은 사용할 클라우드 개발 도구, 플랫폼, 제품을 결정하지 않았음.
	내부적인 클라우드 개발	현재 클라우드 도구, 플랫폼, 제품 사용을 평가하고 기존 사용을 기업 수준으로 확대할지 광범위한 활용을 위해 새로운 접근법을 취할지 결정해야 함.

양호 주의 부적합

녹색 표시는 시정 작업을 포함함

출처: 리미니스트리트

그림 1

고려 요소 2: 통합 관련 리스크 수용도

통합은 하이브리드 IT 환경의 요구사항 중 하나이지만, 데이터 또는 프로세스가 여러 시스템, 제품, 서비스를 거쳐갈 때마다 리스크가 발생합니다. 하이브리드 IT 포트폴리오에는 기업의 통합 관련 리스크 수용도에 따라 다양한 클라우드 공급업체가 포함될 수 있습니다. 데이터 동기화. 데이터 무결성 등과 관련한 다양한 잠재적 이슈에 대한 수용도가 낮은 기업들은 하이브리드 IT에 포함되는 공급업체 수를 낮게 유지해야 하고 중요한 데이터와 프로세스는 클라우드 공급업체보다는 내부적으로 보관하는 편을 선택할 수도 있습니다.

외부적인 관점에서 보면, 조합 속에 파트너사 수가 많을수록 통합 관련 리스크가 더 많아집니다. 비(非) 클라우드 포트폴리오에서 볼 수 있는 리스크와 동일한 리스크도 있습니다. 예를 들면, 데이터 부조화는 데이터 동기화 오류를 발생시킵니다. 클라우드의 서비스 특성에서 비롯되는 리스크도 있습니다. 가령 SLA 간에 부조화가 있는 경우 통합 시점이 비즈니스 방해 리스크가 됩니다. 일부 통합 관련 리스크는 크게 눈에 안 띄면서도 비즈니스 운영에는 큰 지장을 초래하기도 합니다. 변경 적용 시간대 조합이 잘못되는 경우 변경 이벤트 시간 동안 데이터 동기화 리스크가 발생하는 것이 그 예입니다.

내부적으로 보면, 기업들은 클라우드 내 데이터 및 프로세스 배치에 관한 의사 결정을 내릴 때나 이런 결정을 다양한 클라우드 서비스에 걸쳐 적용할 때 수용 가능한 통합 리스크 수준을 정해야 합니다. 하이브리드 IT 포트폴리오에 숙고를 거친 일관성 있는 원칙을 적용하면 데이터가 적시에 안전하게 흐를 수 있게 하는 끊김 없는 통합이 가능하게 되어 비즈니스에도 이점을 가져다 주고 프로세스 무결성 역시 기업이 감수할 수 있는 리스크 수준에서 유지될 수 있습니다.

조언:

- **수용 가능한 통합 관련 리스크를 결정하기 위한** 기본 원칙을 수립하세요.
- **이러한 기본 원칙을 바탕으로 솔루션 선택과 데이터 관리 과정에서 통합 체크리스트를 활용하여** 다양한 공간에 데이터를 배치함으로써 발생할 수 있는 잠재 이슈와 이슈 발생시 리스크 수준을 식별하세요. 그림 2에서 통합 체크리스트 예시를 확인하세요.
- **프로레스가 여러 솔루션을 지나갈 때** 현재 프로세스 무결성 통제 장치가 무효화될지 새로운 통제 장치가 필요할지 판단하세요.
- **비즈니스에 중요한 정도, 시간에 종속된 정도, 민감도, 컴플라이언스 제약이 있는 정도 등의 여러 기준을 바탕으로 다양한 유형의 데이터와 프로세스에 적용되는** 여러 리스크 수준을 가늠해 보세요. 통합 체크리스트에 시점과 보안성에 관한 요소를 포함하여 다양한 시스템을 아우르는 운영에서 발생하는 리스크의 수준을 파악하세요. 리스크 요소에는 기술, 데이터, 비즈니스 프로세스 리스크는 물론 제품 및 공급업체 차원의 리스크도 포함되어야 합니다.

하이브리드 IT 통합 관련 리스크 요소에 대한 초보자용 체크리스트

통합 리스크 구분	리스크 요소
데이터	■ 하이브리드 환경에 걸친 데이터 중복이 식별되고 관리 가능함 ■ 하이브리드 환경에 걸쳐 데이터 정의가 일치하고 불일치하는 정의는 수용 가능함 ■ 데이터 단절이 파악되며 완화 계획이 마련되어 있음(예: 수신 솔루션에는 필요하지만 전송 솔루션에서는 사용 불가한 경우) ■ ABC사에는 데이터 관리 팀이 운영 중이며 클라우드 구현에 적합하지 않은 민감한 데이터와 프로세스를 식별함
프로세스	■ 하이브리드 통합 프로세스들(내부적으로 구현된 환경과 클라우드 환경을 모두 거치는 프로세스)에는 공백이나 겹치는 단계가 없으며, 불일치 사항은 식별되고 수용 가능함
애플리케이션	■ 애플리케이션 아키텍처가 호환 가능함(예: 마스터 파일 구성이 모든 솔루션에 걸쳐 일치)
보안	■ 전사 보안 정책을 클라우드 기반 데이터 및 프로세스에 적용할 수 있음
통합 역량	■ ABC사 내 전사 차원의 통합 관련 팀이 존재함 ■ 통합 역량 조직이 존재함 ■ 클라우드 통합 관련 프로세스와 책임이 정의됨 ■ 클라우드 통합 관련 정책이 마련됨

출처: 리미니스트리트

그림 2

고려 요소 3: 하이브리드 IT 환경 보안

외부적인 관점에서 보면, 클라우드 환경에서 보안 프로세스, 통제 장치, 거버넌스는 여전히 진화 중입니다. 하이브리드 IT 환경도 마찬가지입니다. 경우에 따라서는 기존에 수립된 것이 고객에게는 불리하게 작용하기도 합니다. 예를 들어 SaaS 환경에서는 소프트웨어 공급업체가 완성형 서비스를 제공하기 때문에 고객은 클라우드 보안이 어떻게 유지되는지 알 수 없습니다. 보안에 대한 이해는 기업이 클라우드 공급업체의 손에 맡길 데이터 유형을 결정하는 데 필요할 수 있습니다. 이러한 가시성 없이는 기업 데이터의 보안성이 충분히 지켜질지 파악하기가 어렵습니다.

보안 통제 장치를 공개하지 않는 정책은 대다수 SaaS 공급업체에서 일반적으로 찾아볼 수 있는 운영 절차입니다. 대부분 클라우드 공급업체는 자사가 규정 및 지침을 준수하고 있음을 증명할 것입니다(가령 보안 통제 장치에 대한 정보를 제공하는 대신 자사가 결제 데이터 보안(PCI)을 지키고 있음을 증명). 기업이 공급업체가 제공하는 환경의 안전성과 보안성을 향해 구축하는 신뢰 수준은 클라우드에 맡길 요소를 결정하는 데 영향을 미쳐 결국에는 하이브리드 IT 환경을 결정짓게 될 것입니다.

내부적으로 보면, 기업이 하이브리드 IT 환경 보안을 위해 추가적인 행동을 취할 의향과 역량을 모두 갖춰야 합니다. 데이터를 예로 들면, 클라우드 내 권한 관리는 기업이 데이터를 사용하거나 보호해야 하는 방식과 일치하지 않을 수 있습니다. 특히 보안 수준이 공급업체별로 다른 경우라면 적절한 데이터 보안을 위해 데이터 초크 포인트(choke point)에 명확하고 구체적인 통제 장치가 필요합니다. 하이브리드 IT 환경 제공과 하이브리드 환경 전반에 걸친 견고한 보안성 확보를 위해서는 클라우드와 비(非)클라우드 환경을 이해하는 강력한 내부 보안팀이 필수입니다. 사내 보안팀의 역량은 클라우드 안에 안전하게 배치될 수 있는 기술에 영향을 미쳐 하이브리드 IT 포트폴리오를 구체화할 것입니다.

조언:

- **클라우드 공급업체와 상호 신뢰와** 좋은 관계를 구축하세요. 가능한 수준까지 클라우드 서비스 내부에 대한 이해를 넓혀 공급업체가 취약해 보이는 지점을 내부적으로 견제할 수 있도록 하세요. 신뢰 수준이 낮다면 기업의 "비법"이나 중요 데이터를 클라우드에 저장하지 마세요.
- **보안 정책을 수정하여** 내부 플랫폼과 클라우드 플랫폼 전반에 걸쳐 일관성을 확보하세요. 하이브리드 IT 보안의 상당 부분은 여전히 기업의 책임입니다. 예를 들면 데이터가 보관되거나 전송되는 각 위치에서의 보안은 일관성이 있어야 합니다.
- **클라우드 및 비클라우드 매트릭스를 생성하여** 기업이 보안을 책임져야 하는 시스템을 명확하게 설정하세요. 그림 3에서 하이브리드 IT 보안 책임 예시를 확인하세요.
- **하이브리드 IT 환경 중 클라우드 부문과 이를 담당하는 데 적합한 인력에 대한** 통제 조치를 설정하세요. 앞서 든 데이터 예시에서 데이터 손실 방지(data loss prevention, DLP) 솔루션은 민감한 데이터가 실수로 클라우드로 흘러들어가지 않도록 할 수 있습니다. 하지만 충분한 통제책을 보장할 수 없다면 기술을 클라우드로 이관하지 않는 게 좋습니다.
- **각 클라우드 공급업체의 온보딩에** 보안 관련 역할과 책임 식별을 포함하세요.

하이브리드 IT 보안 책임 예시

출처: 리미니스트리트

그림 3

하이브리드 IT 환경의 모습은 우연이 아닙니다.

이와 같은 3대 핵심 요소를 모두 고려하여 하이브리드 IT 모델을 전략적으로 구축하세요. 하이브리드 IT 포트폴리오에서 클라우드 부문은 "서비스로서의(as-a-service)"라는 개념이 실질적으로 비즈니스 가치를 가져다주는지에 따라 결정하세요. 이와 동시에 통합 리스크를 항상 낮은 수준으로 유지하면서 환경의 보안성을 유지하세요. SaaS, 플랫폼, 도구의 선택지를 조율하여 민첩성과 유연성을 확보하세요. 마지막으로 특히 신뢰, 투명성, 통제 장치 요소와 관련해 공급업체가 실패할 가능성을 관리하기 위한 종합 계획을 수립하세요.

관련 자료에서 하이브리드 접근법 수립에 대한 자세한 내용을 확인하세요: "하이브리드 IT를 통한 디지털 혁신 지원"

Rimini Street®

riministreet.com/kr
enquirykorea@riministreet.com
twitter.com/riministreet
linkedin.com/company/rimini-street

리미니스트리트(Nasdaq: RMNI)는 엔터프라이즈 소프트웨어 제품 및 서비스를 제공하는 글로벌 기업으로, 오라클 및 SAP 소프트웨어 제품에 3자 유지보수 서비스를 제공하며 Salesforce®파트너 업체이기도 합니다. 당사에서는 대응 능력이 극히 뛰어난 최고급 통합형 애플리케이션 관리 및 유지보수 서비스를 제공하여 엔터프라이즈 소프트웨어 라이선스 사용 기업에서 비용을 대폭 절약하고 혁신을 위한 여유 리소스를 확보하며 더 나은 비즈니스 성과를 올릴 수 있도록 지원합니다. 글로벌 포춘 500대 기업, 중견기업, 공공 부문은 물론 다양한 업종의 기타 기업 조직과 단체에서도 리미니스트리트를 엔터프라이즈 소프트웨어 제품 및 서비스 제공업체로 믿고 의지하고 있습니다.

© 2021 Rimini Street, Inc. All rights reserved. '리미니스트리트'는 미국 및 기타 국가에서 리미니스트리트의 등록상표이며 '리미니스트리트'와 그 로고 및 이 둘의 조합과 TM이 표시된 기타 기호는 모두 리미니스트리트의 상표입니다. 기타 모든 상표는 각 소유주의 재산이며, 달리 명시된 경우를 제외하고 리미니스트리트는 본문에서 언급한 모든 상표 소유자 또는 기타 업체와의 제휴관계, 홍보 또는 연관관계를 주장하지 않습니다. 본 문서는 리미니스트리트 주식회사(이하 '리미니스트리트')에서 제작되었으며, 오라클, SAP SE, 또는 기타 관계자의 후원이나 지지를 받거나 제휴관계에 있지 않음을 밝힙니다. 달리 서면으로 명확하게 제시한 경우를 제외하고, 리미니스트리트는 본문에 제시된 정보와 관련하여 각종 명시적, 묵시적 또는 법제적 보증에 대해 아무런 책임을 지지 않습니다. 여기에는 상업성 또는 특정 용도의 적합성에 대한 암묵적인 보증이 포함되며 이에 국한되지 않습니다. 리미니스트리트는 본문에 제시된 정보를 사용하거나 사용하지 못함으로써 발생하는 각종 직간접적, 결과적, 징벌적, 특수 또는 우발적 피해에 대해 아무런 책임을 지지 않습니다. 리미니스트리트는 제 3자가 제공한 각종 정보의 정확도 또는 완전성과 관련하여 어떠한 의견을 내세우거나 보증을 하지 않으며, 각종 정보, 서비스 또는 제품을 언제든 변경할 권리가 있습니다.
LR-68995 | KR-080921