IDG
STRATEGIC
MARKETING SERVICES

PLATEER

IDG Summary | PLATEER

“강력한 통제와 빠른 개발을 동시에”

강화된 IT 감사에 대응하는 ITSM을 구축하는 방법

무단 전재
재배포 금지

본 PDF 문서는 IDG Korea의 자산으로, 저작권법의 보호를 받습니다.
IDG Korea의 허락 없이 PDF 문서를 온라인 사이트 등에 무단 게재, 전재하거나 유포할 수 없습니다.

“강력한 통제와 빠른 개발을 동시에”

강화된 IT 감사에 대응하는 ITSM을 구축하는 방법

이호현 | 플래티어 수석

오늘날 기업이 처한 어려움은 복합적이다. 코로나19 대유행으로 불확실한 경제 전망이 계속되고 있고, 새로운 경쟁 상황에 더 빠르게 대응하기 위해 디지털 트랜스포메이션을 신속하게 추진해야 하는 숙제도 안고 있다. 여기에 새롭게 부상하는 경영 리스크가 또 있다. 바로 내부회계관리제도다.

내부회계관리제도는 회계 정보 작성 및 공시와 관련해 기업이 지켜야 할 재무보고에 대한 규제다. 재무제표의 오류나 부정, 비리를 막기 위해 재무보고와 관련된 업무를 관리 통제하는 일정 요건의 내부통제시스템을 갖추도록 법률로 강제하고 있다.

현재 이슈가 되는 것은 내부회계관리제도의 주요 원칙 중 하나인 정보기술일반통제(Information Technology General Control, ITGC)다. 법률에는 ‘회사는 내부회계관리제도 목적 달성을 지원하는 정보기술일반통제를 선정하고 구축한다’라고 명시돼 있는데, 여기서 말하는 정보기술일반통제가 바로 IT 관리 인프라다. IT 시스템에서 산출된 정보의 신뢰성을 검증할 수 있도록 지원하는 역할을 한다.

이 법률은 지난 2019년부터 자산규모 2조 원 이상 기업을 대상으로 이미 시행됐다. 2020년에는 자산 5,000억 원 이상으로 확대됐고, 2022년엔 1,000억 원 이상, 2023년에는 모든 기업으로 적용 대상이 늘어난다. 기업이 ITGC에 규정된 시스템을 구축하지 못하면 회계감사 결과에 따라 상당한 불이익을 감수해야 한다. 상장사의 경우 2년 연속 비적정 의견을 받으면 상장폐지 대상이 될 수 있다. 당장 중견 규모 이상의 상장사는 발등의 불이 떨어진 셈이다. ITGC에 대한 대응이 시급한 상황이다.

기존 ITSM이 새 회계관리제도 ITGC에 맞지 않는 이유

ITGC는 결국 IT 시스템의 문제로 재무제표 오류나 부정이 발생할 수 있는 위험요소에 대한 통제력을 갖추는 것이 핵심이다. 예를 들면 시스템이 데이터를 잘못 처리하거나 승인 없이 데이터가 부적절하게 변경될 위험, IT 부서 인원의 업무분담이 적절하지 않거나 부적절한 수작업 혹은 데이터 유실의 위험 등을 효과적으로 관리하고 그 신뢰성을 검증할 수

있어야 한다.

그동안 기업은 이 위험 요소를 관리하기 위해 ITSM(IT Service Management)이나 ALM (Application Lifecycle Management) 시스템을 활용했다. IT의 계획부터 취득/개발, 운영 및 유지보수, 모니터링, 개선까지 전체 수명 주기를 통제하는 솔루션이다. 문제는 기존의 ITSM이 ITGC라는 새로운 상황에 대응할 수 있는지다. 안타깝게도 그 한계가 하나둘씩 드러나고 있다.

가장 심각한 문제는 이른바 '끊어진 링크(missing link)'다. 예를 들어 A기업의 실제 회계 감사 사례를 보자. 몇몇 샘플 데이터를 뽑아 감사에 제출한 데이터대로 진행되는지 기존 ITSM을 이용해 로우 데이터를 분석했다. 그런데 정확하게 이력을 추적할 수 없는 데이터가 무더기로 나왔다. a.java라는 파일을 수정했다고 감사 자료에 제출했는데, 실제 이 작업이 이뤄졌는지 검증할 수 있는 데이터를 제시하지 못했다. 파일의 어떤 부분이 수정된 것인지 정도만 확인하려 했지만, 이 내용도 추적할 수 없었다. 결국 회계감사 지적사항으로 잡혔다.

ITGC의 여러 기능을 서로 연동하는 코어를 구현하는 것도 기존 ITSM 솔루션의 한계다. ITGC에 효과적으로 대응하려면 변경 관리부터 배포, 품질관리 등 애플리케이션의 전체 수명 주기에 맞춰 다양한 기능이 필요하다. 이런 인프라를 구축하는 방법은 IBM이나 마이크로소프트 같은 대형 업체의 상용 통합 솔루션을 도입하거나, 오픈소스를 활용하는 방식 혹은 상용 솔루션과 오픈소스를 필요에 따라 혼용하는 방법 등이 있다.

상용 통합 솔루션은 가장 안정적일 수 있지만 비용 부담이 너무 크다. 특히 개별 기업 상황에 맞춰 기능을 수정, 보완하거나 비용 절감을 위해 오픈소스를 혼용할 경우 서로 연동하는 작업이 필요한데, 이 과정에서 충분한 기술지원을 받지 못할 가능성이 있다.

예를 들어 기업이 ITGC에 대응하기 위해 유명 오픈소스 빌드 솔루션인 젠킨스(Jenkins)를 도입한다고 하자. 빌드 작업은 다른 솔루션의 명령을 받아 작동하므로, 명령을 보내는 솔루션과 젠킨스를 연동하는 작업이 필요하다. 이때 상용 솔루션 업체는 자사의 고가 연동 플러그인을 쓰도록 강요하거나 혹은 기업이 자체적으로 개발해야 한다며 사실상 방치하는 상황이 종종 발생한다. 상용 솔루션 업체는 자사 영업 전략에 따라 기술지원 인력을 운용하는데, 일부 외산 솔루션 업체의 국내 지사는 ITSM 지원 인력 자체가 없는 경우도 있다.

기존 ITSM의 또 다른 치명적인 단점은 최근 주목받는 개발 방법을 수용하지 못한다는 것이다. 오늘날 IT 개발은 프로세스 중심에서 서비스 중심으로 전환해, 잦은 업데이트와 신속한 혁신이 가능하도록 바뀌고 있다. 빠른 시장 변화에 대응해 전체 IT 개발의 속도를 높이려는 기업의 필요를 반영한 것이다. 그러나 기존 ITSM은 변경 관리 수준의 추적성에 초점을 맞추고 있다. 배포 자동화부터 CI/CT/CD, 데브옵스까지 반영한 새로운 ITSM 요건을 지원하지 못한다.

전통적인 ITSM 시스템은 관리에만 중점을 두어 전반적으로 절차가 복잡하다. 워터폴(Waterfall) 기반의 개발이 중심인 기업에는 어느 정도 적합할지 모르지만, 디지털 트랜스포메이션을 추구하는 기업에는 무겁고 불편하다는 인식이 지배적이다. 특히 최근의 서비스 형태는 고객 중심적이고 고객의 요구에 얼마나 빠르게 대응하는지가 기업의 성공과 실패를 가르는 핵심 요소다. 기존의 절차 지향적이고 관리 중심적인 ITSM이 점점 더 외면받는 것도 이 때문이다.

강력한 통제와 빠른 개발을 동시에 구현하는 방법

그렇다면 ITGC 시대에 맞는 새로운 ITSM을 어떻게 구축해야 할까. 해법은 절차의 단순화와 자동화로 압축할 수 있다.

절차의 단순화는 개발 프로세스의 본질에서 출발해야 한다. ITGC 시대라고 해도 설계-개발-테스트-배포로 이어지는 기본적인 프로세스 자체가 바뀌는 것은 아니다. 이 프로세스를 관장하는 ITSM이 복잡하고 사용자의 중복 입력을 요구하면서 점점 더 무겁고 불편해졌을 뿐이다.

따라서 새로운 ITSM은 애자일 등의 방법론을 반영해 가능한 한 개발 프로세스를 간소화해

야 한다. 예를 들면 지라(Jira)와 같은 변경 관리 솔루션은 자체적으로 애자일의 기본 프로세스를 제공한다. 기업이 이 프로세스 가이드를 활용해 현장 업무에 적용하면 개발 프로세스 전체를 축소하고 단순화할 수 있다. 새로운 ITSM 전체를 큰 저항 없이 안정적으로 구축, 운영할 수 있다.

절차를 단순화하기 위해 솔루션이 꼭 지원해야 할 것이 또 하나 있다. 바로 유연성이다. 다시 변경관리를 예로 들면, 이 업무는 기업마다 독자적인 절차가 있는 경우가 많다. 문제는 이런 예외성을 솔루션이 제공하는 기본 애자일 프로세스로 지원할 수 있는지다. A-B-C로 이어지는 워크플로우인데, A-C로 B를 건너뛰거나 혹은 B-C 사이에 팀장 승인 절차를 추가하는 등의 변화를 ITSM에서 구현할 수 없으면 내실 있는 단순화가 아니라 그냥 반쪽짜리 ITSM이 돼 버린다.

자동화는 ITGC의 핵심 요건과 밀접하게 관련이 있다. ITGC는 회계 투명성을 위해 IT 운영에 수작업을 지양한다. A라는 부분을 수정한다고 계획한 후 실제로는 다른 부분을 몰래 수작업으로 바꾸는 문제가 발생할 수 있기 때문이다. A 작업의 신뢰성도 전혀 증명할 수 없다. 이처럼 사람의 수작업이 아니라 시스템에 의한 작업이 이뤄지기 위해서는 자동화가 필수적이다. 수작업을 배제하는 것은 물론, 규제와 정책을 준수하기 위한 데이터를 정확하게 수집, 통제하고 있는지 증빙할 수 있는 자동화여야 한다.

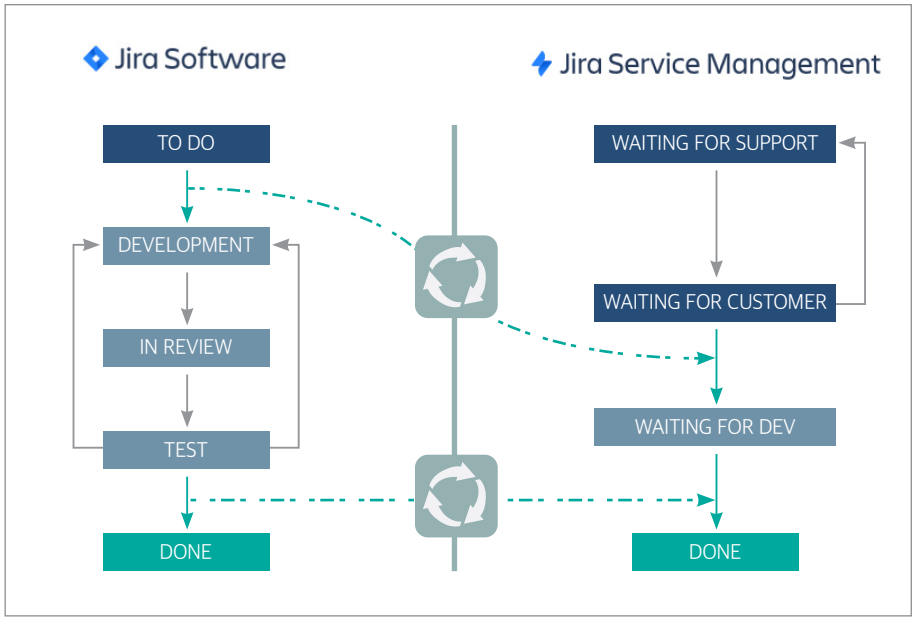
절차의 단순화와 자동화가 솔루션 측면의 해법이라면 ITGC에 대응하는 체계 전체를 완성하는 마지막 조각이 바로 문화와 컨설팅 등 인적 요소다. ITGC와 같은 컴플라이언스 이슈는 솔루션의 문제이면서 동시에 사람의 문제이기도 하다. 아무리 좋은 솔루션도 이를 잘 쓸 수 있는 환경을 마련하고 구체적인 교육과 가이드가 필요하다. 이러한 요소는 단기간에 만들어지는 것이 아니므로 외부 전문가의 도움을 받는 것이 효율적이다.

최종적인 목표는 새로운 ITSM 솔루션을 구축하는 과정의 시행착오를 최소화하고, 구축한 이후에 본래 기대했던 것처럼 잘 활용할 수 있는 문화를 만드는 것이다. 그래야만 기업이 강력한 통제와 빠른 개발을 동시에 만족하는 ITSM을 확보할 수 있다.

ITGC 대응 최적 조합 'JSM 솔루션+플래티어 컨설팅'

플래티어는 기업이 ITGC에 대응할 수 있도록 아틀라시안의 ITSM 솔루션 JSM(Jira Service Management)과 관련 컨설팅을 국내 기업에 공급하고 있다.

JSM이 기존 ITSM과 차별화된 가장 큰 특징은 가시성이다. 보통 업무의 전체 진행 상황을 대시보드 등을 통해 쉽게 확인할 수 없으면 실무자의 기억으로 일정을 관리하게 된다. 이



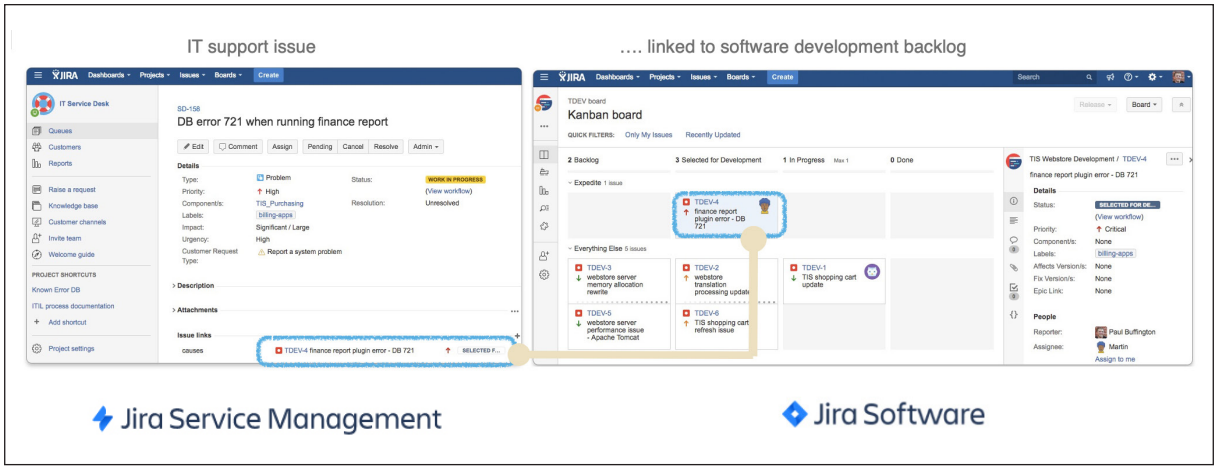
JSM을 이용하면 변경 관리를 ITSM에 연동할 수 있다.

과정에서 업무 처리가 늦어지거나 차질이 발생할 가능성이 크다. 반면, JSM은 미리 정해진 SLA(Service Level Agreement) 기간 안에 처리하지 못하면 알림을 보낸다. 팀원 전체의 업무 현황과 업무량을 한 번에 볼 수 있으므로 문제가 발생하기 전에 합리적으로 업무를 재분배할 수 있다. 이미 수정된 파일을 검토하지 않아 생기는 프로세스상의 병목도 바로 알 수 있어 더 속도감 있게 협업할 수 있다.

유연성도 JSM의 강점이다. 많은 기업이 ITSM을 내부에서 직접 개발하거나 ITSM 솔루션을 커스터마이징해 구축한다. 그러나 이런 방식은 민첩성이 떨어지기 쉽다. 중간에 팀장 승인 절차를 추가하는 등 변경할 부분이 생길 때마다 개발팀이 투입돼 작업해야 하기 때문이다. 반면 JSM은 마치 다이어그램처럼 화면에서 쉽게 박스를 옮기는 것으로 절차를 추가, 수정할 수 있다. 전체 개발 과정을 한 화면에서 보면서 화살표로 연결해 업무 절차를 조정하거나 추적하는 것도 가능하다.

JSM은 현재 ITIL(IT Infrastructure Library) v4를 지원하는 거의 유일한 ITSM 솔루션이다. ITIL이란 ITSM의 베스트 프랙틱스로, v4는 지난해 발표됐다. v4가 v3과 가장 크게 달라진 점은 최근의 개발 방법 변화를 반영해 애자일과 데브옵스, 디자인씽킹 등을 수용한 것이다. 이제 JSM내에서 ITIL v4 프로세스를 기본으로 제공하므로 기업은 이를 가이드로 활용해 최신 개발 방법을 도입할 수 있다.

한편 JSM 솔루션의 효용을 극대화하는 것이 플래티어의 컨설팅이다. 플래티어는 프로세스부터 툴, 문화, 실행 단계까지 기업이 ITSM을 구축, 운영하는 과정에서 겪는 다양한 시행



JSM을 이용하면 회계 보고서 플러그인의 문제를 담당자에 할당해 지속적으로 추적할 수 있다.

착오에 대한 해법을 제공한다. 이런 지원이 가능한 것은 플래티어가 전문 인력을 충분하게 보유하고 있기 때문이다. 현재 플래티어에는 경력 15년이 넘는 컨설턴트가 다수 포진해 있다. 국내에서 가장 큰 규모로 전문가를 확보한 기업 중 하나다.

감사 대응 작업 시간을 1달에서 5분으로

JSM 솔루션과 플래티어 컨설팅을 결합해 ITGC에 잘 대응한 대표적인 성공 사례가 국내 제조 기업인 A사다.

기간 산업계로 분류되는 이 기업은 ITGC에 따른 회계감사의 리스크를 충분히 인식하고 있었다. 일단 라인이 멈추면 막대한 손실이 발생하는 업종 특성상, 규제가 없다고 해도 모든 IT 산출물을 정확하게 검증해 배포해야 하는 내부적인 필요도 있었다. A사는 ITGC에 대응하기 위해 JSM 등 아틀라시안이 개발한 툴을 활용해 ITSM 시스템을 구축했다. 회계감사를 대비해 로우 데이터를 수집할 수 있는 내부 솔루션도 개발했다.

그 결과 감사 과정에서 요구하는 데이터를 추출하는 작업 시간을 획기적으로 단축했다. 이 시스템을 구축하기 전에는 모든 데이터를 문자 그대로 일일이 작업해야 했다. 각 시스템에서 필요한 데이터를 찾아 다운로드하는 방식이었다. 이 작업에만 1달 이상이 걸렸다. 하지만 현재는 표준화된 ITGC 정책에 의한 운영 관리가 가능하다. ITGC 모니터링 시스템에서 시스템 별 조건, 범위를 설정하면 감사 데이터를 빠르면 5분 만에 수집해 다운로드할 수 있다. A사는 ITGC 대상 시스템을 점차 확대하고 있다.

이러한 시스템 투자에 대한 경제적 효과는 단순 계산으로도 바로 확인할 수 있다. 기존 방식으로는 회계감사에 대응을 위해 각 시스템마다 근거 자료를 추출하는 작업 공수가 소요됐다. 가능한 한 내부 인력으로 처리하지만, 필요시 데이터 수집 인력을 추가로 투입하는

상황이 발생했다. 이런 외부 전문 인력 비용을 1인당 월 1,000만 원으로 계산하면 시스템 1대당 길게는 2개월, 총 2,000만 원이 들어간다. ITGC 대상 시스템이 100대 이상인 대기업이라면 ITGC 대응에만 20억 원 이상이 필요하고 이를 매년 반복해야 한다. 결국 자동화와 수작업을 비교하면 어떤 기준으로 판단해도 JSM을 활용하는 것이 이익이다.

더구나 JSM를 활용했을 때의 장점은 정확하다는 것이다. 사람이 직접 회계 감사 데이터를 수집하면 이 과정에서 인적 실수, 이른바 '휴먼 에러'가 발생할 가능성이 있다. 반면 자동화된 ITSM 솔루션을 이용하면 필요한 데이터를 실수 없이 빠르게 추출할 수 있다.

시작하는 기업을 위한 2단계 ITSM 구축 가이드

현재 국내에서 ITSM 고도화를 추진하는 기업은 A사 뿐만이 아니다. 2023년에는 자산 규모와 관계없이 ITGC가 적용될 예정이어서, 시기의 문제일 뿐 모든 기업이 ITGC에 대응할 수 있는 ITSM을 새로 도입하거나 기존 ITSM을 개선해야 한다. 특히 포털과 게임 등 IT 기업은 앞으로 회계감사에서 회사 운영보다는 ITGC 대응 체계를 중심으로 감사를 받게 될 가능성이 크다. 바꿔 말하면 ITSM을 도입했을 때 단기간에 효과를 체감할 수 있는 산업군이라는 의미이기도 하다.

ITGC에 대응할 수 있는 ITSM 구축 필요성을 인식했다면 구체적으로 어떻게 시작해야 할까. 이때는 먼저 관리할 대상을 명확히 인식하고 그 후에 이를 지원하는 솔루션을 도입하는 2단계 구축 전략을 추천한다.

흔히 많은 기업이 ITGC에 대응하는 솔루션을 구매하면 단번에 문제가 해결되리라 생각한다. 그러나 현실에서는 전혀 그렇지 않다. 솔루션만 도입하고 이를 운영하기 위한 교육이나 문화, 프로세스를 함께 만들지 않으면 비용은 비용대로 쓰고, 감사 대응은 수작업으로 하면서 결국 수많은 지적사항을 떠안는 최악의 상황에 놓일 수 있다.

이런 불상사를 피하기 위해서는 먼저 ITGC 규정을 확인해 이를 충족하기 위해 기업 내부에서 어떻게 해야 할지 고민할 필요가 있다. 이를 통해 구체적으로 증빙해야 할 대상을 특정할 수 있다. 작은 규모라도 ITGC 증빙에 필요한 데이터를 직접 뽑아보면 어떤 항목에 대응해야 하는지 더 정확하게 파악할 수 있다. 이런 증빙 작업까지 순조롭게 진행했다면 구체적인 자동화 솔루션을 검토하고 도입 계획을 수립하면 된다.

이러한 2단계 전략은 정확하게 2개 솔루션에 직접 대응된다. 1단계가 변경 관리 솔루션, 2단계가 자동화 솔루션이다. 변경 관리는 누가 어떤 작업을 언제까지 했는지에 대한 이력을 관리, 추적하는 것이다. ITGC 감사에서 특정 변경 작업에 대한 근거를 요구할 때 바로

참조할 수 있다. 변경 관리를 통해 기업은 감사에 대비해 증빙해야 할 작업이 무엇인지 정확하게 인식할 수 있다. ITGC 시대의 ITSM을 구축하는 출발점이 변경 관리인 이유다. 현재 가장 널리 쓰이는 변경관리 솔루션 중 하나가 아틀라시안의 '지라'다.

변경 관리가 어느 정도 자리를 잡으면 이제 2단계로 변경 관리 증빙 작업을 더 효율적으로 처리하는 방법을 찾아야 한다. 바로 자동화다. 수작업에 따른 실수를 없애고 작업 시간을 최소화하기 위해 필수적이다. 이 자동화를 담당하는 아틀라시안의 대표적인 솔루션이 앞서 살펴본 'JSM'이다. 이미 선도적인 기업은 변경 관리를 안정적으로 운영하고 있고, 현재는 ITGC에 대응하기 위해 자동화 단계로 넘어가고 있다.

기업이 이런 작업을 진행할 때는 외부 전문가와 협업하는 것도 좋다. 개별 기업의 워크 플로우에 맞는 솔루션을 제안받는 것은 물론 프로세스 표준화에 대한 조언까지 얻을 수 있다. 특히 고가의 상용 통합 솔루션 대신 유연하고 비용 면에서도 효율적으로 오픈소스와 상호 호환성이 높은 솔루션 도구에 관심이 많고 기업 내부에 숙련된 실무자가 부족하다면, 솔루션 검토부터 도입, 구축, 기술 지원 등을 제공할 수 있는 노련한 전문 컨설팅 업체와 협업할 필요가 있다.

ITGC라는 치명적인 경영 리스크에 대응하려면

기존 ITSM 환경은 정형화돼 있고 복잡한 구조를 가진 한계가 있었다. 이제 ITGC라는 새로운 규제 환경에 맞춰 ITSM은 더 단순해져야 한다. 동시에 애자일, 데브옵스 등 최근 개발 패턴에 최적화해 강력한 통제와 빠른 개발을 동시에 지원할 수 있어야 한다. 이는 ITGC라는 치명적인 경영 리스크에 효과적으로 대응하는 것은 물론, 오늘날 기업의 최대 과제인 디지털 트랜스포메이션에 성공하는 지름길이기도 하다.