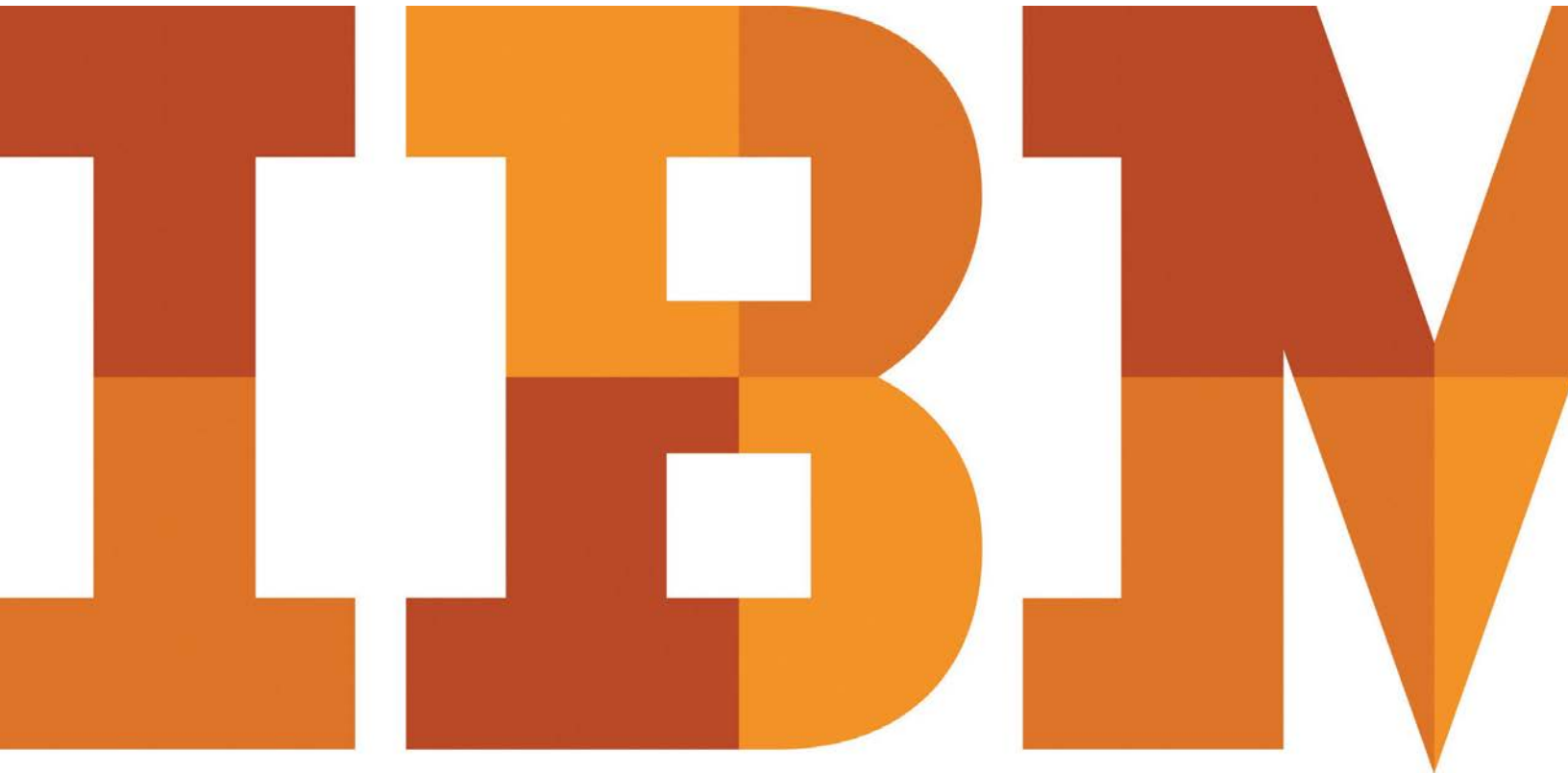


# ID(Identity) 및 액세스 관리를 통해 지속적인 규정 준수와 리스크 완화 실현

*자산, 애플리케이션, 정보에 대한  
사용자의 액세스 관리, 제어 및 모니터링*



## 주요 내용

- 자산에 액세스하는 모든 사용자의 자격 검증
- 사용자 액세스가 해당 사용 정책을 따르며 규정을 준수하는지 여부 모니터링
- 위반 발생 시 시정 조치 실행
- 사용자 라이프사이클 전반에서 사용자 권한 부여에 대한 신뢰성 및 투명성 보장
- 사용자의 활동을 지속적으로 감사(audit)하여 정책과 규정 준수

사용자에게 더 우수한 품질과 가용성의 서비스를 안정적으로 제공하는 데 있어, 비용 관리와 액세스 지점, 애플리케이션, 사용자 수의 변동은 기업이 해결해야 할 과제입니다. 하지만 ID 및 액세스 관리(Identity and Access Management, IAM) 측면에서 보자면 이는 일부에 불과한 문제입니다. 서비스는 직원, 공급자, 파트너, 고객을 불문하고 적합한 권한을 가진 올바른 대상에게 전달되어야 합니다. 이러한 과제는 날이 갈수록 그 중요도가 더해지고 있으나, 기업이 해결하기는 쉽지 않습니다.

SOX(Sarbanes-Oxley), Basel II, 개인정보보호법, 정보통신망법, 전자금융감독규정, PCI/DSS (Payment Card Industry Data Security Standard)와 같은 규정들은 사용자 자격과 액세스 권한의 감시 및 제어에 무게를 두고 있습니다. 또한, 컴퓨팅의 발전에 따라 다음과 같은 어려움이 가중되고 있습니다.

- 정형 데이터 및 비정형 데이터의 폭발적 증가
- 정보에 대해 공간의 제약 없이 액세스
- 클라우드 컴퓨팅과 인터넷 기반의 협업 활성화

IAM의 복잡성, 리스크 및 규정 준수 요건의 압박은 새로운 방식을 요구하고 있으며, 이 새로운 방식을 실현할 솔루션이 기업에 필요합니다. 즉, 생산성의 저하 없이 더 우수한 가시성과 제어, 자동화를 제공하여 무단 액세스로부터 자산을 보호하는 정책 기반의 IAM 거버넌스가 필요합니다.

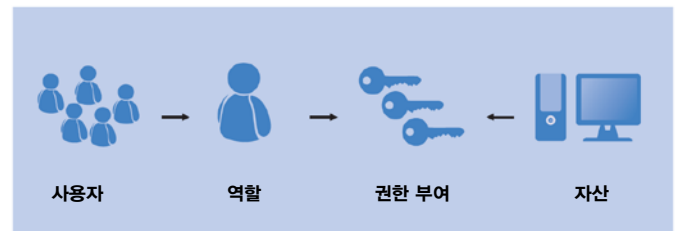


그림 1: IAM 거버넌스는 적합한 권한을 가진 올바른 대상에게 적합한 자산을 제공하도록 지원합니다.

## IAM 거버넌스를 통해 비즈니스의 최전선 방어 구축

IAM 거버넌스는 기업 보안의 최전선에 있습니다. 이는 누가, 어떤 자산을, 어떤 목적으로, 얼마 동안 액세스하도록 승인 받았는지를 파악하기 위한 기본적인 기술입니다. IAM 거버넌스에는 액세스 권한 부여, 갱신, 삭제를 위한 기술 및 정책과 함께, 사용자가 액세스 권한을 가지고 어떤 작업을 하는지 모니터링, 감사, 보고하는 툴이 포함되어 있습니다. IAM 거버넌스가 없으면 권한 부여 관리, 데이터 유출 방지, 사기 탐지와 같은 보안 전략에 액세스 정책을 적용하는 것이 어려워집니다. 또한, IAM 거버넌스는 보안 인텔리전스를 통해 비즈니스 보호를 최적화하기 위한 기본적인 요소이기도 합니다.

많은 기업들이 보안 툴과 기술에 투자를 해 왔습니다. 그러나 계층적인 방어 시스템을 구축하는 것은 기존 환경에 보안 인텔리전스를 구현하는 것과는 차이가 있습니다. 리스크 관리를 보안 체계에 통합하는 사전 예방적 보안도 필요합니다. IBM IAM 거버넌스가 바로 이러한 문제를 해결할 수 있도록 지원합니다. IAM 거버넌스는 사용자 라이프사이클 전반에서 사용자 권한 부여에 대한 신뢰성과 투명성을 실현함으로써 기업이 리스크를 극복하여 가치를 얻을 수 있도록 합니다.

ID 관리를 비즈니스 목표 및 우선 과제와 더 직접적으로 통합함으로써 기업은 각 사용자에게 적합한 IT 서비스를 제공할 수 있으며, 궁극적으로 비즈니스 기회를 더 잘 활용할 수 있습니다. IAM 거버넌스 솔루션은 각종 보안 및 정책 관리 기술을 강화해주며, 통합적인 보안 관리를 향상시킵니다.

IAM 거버넌스는 애플리케이션, 정보, 시스템에 대한 ID와 액세스 권한을 관리, 보호하고 감시할 수 있도록 지원합니다. 또한, 기업이 사용자 프로비저닝, 웹 액세스 관리, 디렉토리 인프라와 같은 ID 및 액세스 관리 기능으로 더 큰 가치를 얻을 수 있도록 돕습니다.

IAM 거버넌스 솔루션은 워크플로우, 보고 툴 및 분석 기술에 기초하여 사용자 액세스를 검색, 분석하고 설정합니다. 기업은 이를 기반으로 권한 부여를 제어할 수 있으며 사용자 액세스 거버넌스 프로세스를 통해 비즈니스 충돌을 해결할 수 있습니다. IAM 거버넌스에는 다음과 같은 프랙티스가 포함됩니다.

- 사용자 라이프사이클 관리(사용자 프로비저닝 및 디프로비저닝)
- 애플리케이션 암호 관리 및 SSO(Single Sign-On), 셀프서비스 옵션으로 헬프데스크 업무량을 줄임
- 역할 관리(사용자의 직무 및 비즈니스 요구 사항에 따라 역할 배정, 임무 분할의 충돌 관리)
- 인증 정책을 통해 정기적인 검토 프로세스를 마련하고 사용자 액세스의 적합성 여부를 검증
- 액세스 관리 - 내부 사용자 및 외부 사용자(예: 비즈니스 파트너, 외부 서비스 제공업체)를 대상으로 정책 기반 액세스 적용
- 권한 부여 관리(역할, 규정, 속성을 세분화하고 이를 기반으로 애플리케이션 및 서비스에 액세스)
- 지속적인 감사 및 보고 - 사용자 활동 모니터링, 정책 적용, 규정 준수 지원

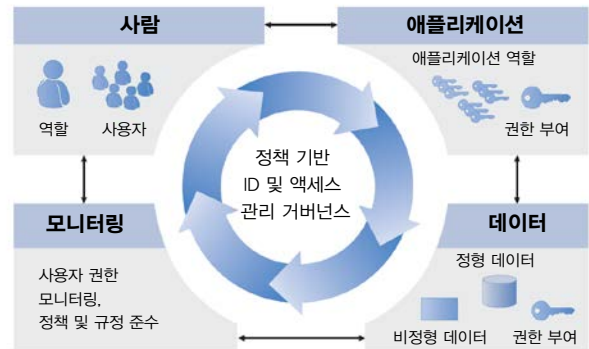


그림 2: IBM은 정책에 기초한 IAM 거버넌스 방식을 지원합니다.

### 정책 기반 IAM의 일관성 실현 및 규정 준수

보안 및 개인 정보 보호에 대한 우려가 높아지고, 규정 준수와 기업 관리에 많은 관심이 모아지고 있는 지금, 데이터 및 애플리케이션에 대한 액세스 제어는 기업에 있어 필수적인 요소가 되었습니다. 기업은 강력하고 일관된 액세스 제어를 구현해야 하며, 비즈니스 목표 및 정책에 따라 사용자 권한 부여를 결정해야 합니다. IBM IAM 거버넌스는 더 우수한 신뢰성과 투명성으로 사용자 액세스 요구 사항을 관리할 수 있는 자원을 제공하며, 더 효과적인 사용자 액세스 관리와 적용을 지원합니다. 정책에 입각하여 사용자, 애플리케이션 및 데이터를 관리하는 IBM의 방식은 효과적인 IAM 거버넌스를 위한 일관성과 다양성을 제공하며 규정 준수도 보장합니다.

IBM은 다음과 같은 5단계 IAM 라이프사이클을 포괄하는 검증된 정책 기반 방식을 제공합니다.

- 관리 항목 정의
- 사용자 등록 및 향후 지원
- 사용자 권한 부여 및 관리

- 액세스 제어 관리 및 실행
- 사용자 권한 및 활동 모니터링, 감사, 보고

각각의 단계에서 고객은 IBM IAM 거버넌스 솔루션을 통해 서비스를 개선하고, 비용을 줄이고, 더 효과적으로 리스크를 관리하면서 비즈니스 가치를 창출할 기회를 누릴 수 있습니다. IBM의 IAM 거버넌스 솔루션은 효율적이고 규정에 부합하는 방식을 통해 적시에 올바른 대상에게 적합한 자산에 대한 액세스 권한을 제공할 수 있도록 합니다. 이는 사용자 인증의 능률화, 애플리케이션 액세스 최적화, 사용자 프로비저닝 및 디프로비저닝 활동의 관리를 통해 이루어집니다. 고객은 IBM의 수준 높은 보안 전문성을 활용하면서 각종 보안 구성요소를 지원 및 개선하고 규정 준수, 사용 정책, 보고 등의 효율성을 높여주는 통합적인 IAM 솔루션을 구축할 수 있습니다. IBM IAM 거버넌스는 사용자 라이프사이클 관리를 간소화하고 사용자 권한 부여에 대한 가시성을 높임으로써 IT 팀의 업무 생산성을 극대화하고 보안 및 규정 준수에 따른 비용과 복잡성의 부담을 최소화합니다.

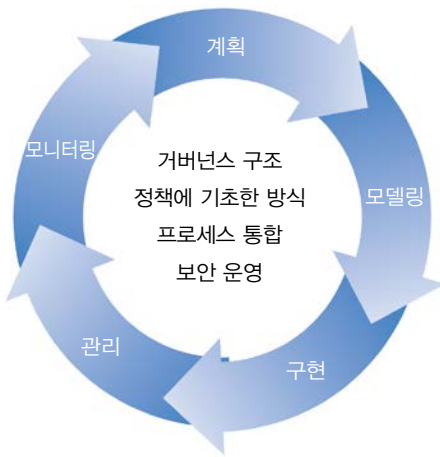


그림 3: 효과적인 IAM 거버넌스 계획은 단단계 폐쇄 루프형(closed-loop) 프로세스를 기반으로 합니다.

### IBM IAM 거버넌스 솔루션

각종 규정과 규제들은 데이터 액세스 및 관리의 신뢰성을 보장해야 할 필요성을 증가시키고 있으며, 이에 따라 기업들은 IAM 기술을 도입하고 있습니다. IAM은 사기를 방지하고 운영 효율을 개선하는 데에도 효과적입니다. 일관적인 관리 방식을 통해 기업은 데이터 무결성을 지키고 규정을 완벽하게 준수할 수 있으며, 클라우드 기반 사용자 커뮤니티, 방대한 데이터 저장소, 모바일 사용 증가에 따른 복잡성도 극복할 수 있습니다. IBM IAM 거버넌스 솔루션을 이용하면 애플리케이션과 데이터를 보호할 수 있고 사용자가 업무상 필요한 자산에 대한 액세스 권한을 신속하게 받을 수 있습니다. IBM IAM 거버넌스 솔루션은 다음과 같은 기능을 제공합니다.

#### ID 관리

ID 관리는 사용자 식별, 사용자 액세스 제어, 사용자 권한 결정 및 관리 권한 위임에 쓰이는 정보를 관리하는 프로세스입니다. 일반 사용자에 대해 이러한 프로세스를 일률적으로 적용하기는 어렵습니다. 각자의 역할과 책임이 자주 바뀌고 사용자 라이프사이클이 계속 변화하기 때문입니다. 직원이 새로운 책임을 맡거나 부서를 옮길 경우, 해당 직원의 액세스 권한을 검토, 승인 및 갱신해야 합니다. 이때 이전의 액세스 권한은 중지되거나 삭제될 것입니다. 고객 액세스 프로필도 바뀔 수 있습니다. 예를 들어, 경매 사이트의 파워 셀러(power seller) 또는 주식 투자자가 지정된 거래량 기준에 도달하면 그 프로필과 권한도 갱신되어야 합니다.

권한 부여에 있어 속도는 정확도 못지않게 중요합니다. 신입 직원이 비즈니스 또는 이메일 애플리케이션에 액세스하지 못하면 아무 일도 하지 못하고 시간만 허비하게 될 것입니다. 클라우드 기반 고객 커뮤니티 및 사용자는 자산에 즉시 액세스할 수 있기를 원합니다.

보안 정책 또한 끊임없이 변하고 있습니다. 따라서 ID 관리 솔루션에는 원활한 정책 수립을 지원하면서 관리자가 정책의 변경을 프로덕션 환경에 적용하지 않고도 잠재적 영향을 평가할 수 있는 툴이 포함되어야 합니다. 규정 준수 및 관리 감독의 차원에서도 ID 및 액세스 데이터를 관리하는 기능이 필요합니다. 사전 정의된 보고 및 감사 이벤트는 감사 담당자가 기업의 보안 실태와 규정 준수 상황을 정확하고 신속하게 파악하는 데 도움이 됩니다.

IT 인프라의 전반에서 정책에 기초하여 사용자와 그 역할을 관리하는 Tivoli® Identity Manager는 ID 및 액세스 거버넌스를 실현하는 핵심 요소 중 하나입니다. Tivoli Identity Manager를 사용하면 사용자 라이프사이클의 전반에서 사용자 권한의 생성, 수정 및 종료 자동화할 수 있습니다. 여기서는 사용자 자체 관리(self-care), 사용자 계정 프로비저닝 및 디프로비저닝, 재인증과 같은 기능이 제공됩니다. 역할 및 정책 모델링 기능은 역할 마이닝 및 모델링, 임무 분할, 그룹 관리를 통해 종합적인 라이프사이클 관리를 실현하며, 다양한 액세스 시나리오의 시뮬레이션도 지원합니다.

#### 액세스 관리

액세스 관리 기능은 엔터프라이즈 시스템 전반에서 일관적인 액세스 제어 정책을 보안 정책 및 규정 요건에 연계하여 관리하며, 여기에는 정책 관리, 모니터링, 적용이 포함됩니다.

액세스 관리 솔루션은 허가 받은 사용자의 일상적인 자산 사용을 관리합니다. 이 효과적인 솔루션을 통해 공식적인 보안 정책을 액세스 관리 워크플로우에 통합할 수 있으며 운영 체제, 네트워크, 서버, 스토리지 장치, 데이터베이스, 데스크탑 애플리케이션, 온라인 거래 시스템, 엔터프라이즈 애플리케이션에 대한 액세스 관리를 자동화할 수 있습니다. 액세스 관리는 사용자가 각종 자산과 애플리케이션에 사용하는 수많은 사용자 이름과 암호를 하나의 강력한 보안 인증 및 승인 프로세스로 통합하며, 여기에는 주로 SSO 기술이 활용됩니다.

액세스 관리 기능은 사용자 라이프사이클의 전반에 액세스 정책을 적용합니다. 즉 여러 환경과 보안 영역에서 사용자를 인증하고, 허가 받은 사용자에게 액세스 권한을 부여합니다. 또한 보안 정책을 적용하고 사내외 위협으로부터 안전하게 보호합니다. IBM의 액세스 관리 제품은 여러 애플리케이션 및 사용자 간에 일관된 보안 정책이 적용되도록 지원하며, SSO를 활성화하여 사용자 환경을 개선하고 헬프데스크 비용을 줄입니다. 권한 부여 관리는 더 세분화된 액세스 권한의 적용을 가능하게 합니다.

IBM은 다음과 같은 IBM IAM 거버넌스 제품을 공급합니다.

- e-비즈니스를 위한 IBM Tivoli Access Manager – 웹과 각종 애플리케이션을 위한 인증 및 권한 부여가 이루어지는 허브로 동작합니다. 액세스 관리를 중앙화하며, 더 쉽고 경제적인 보안 애플리케이션 배포를 지원합니다.
- 엔터프라이즈 SSO(Single Sign On)를 위한 IBM Security Access Manager – 강력한 인증, 액세스 워크플로우 자동화, 빠른 사용자 전환 및 감사 보고 기능과 전사적 SSO 기능을 통합함으로써 액세스 관리를 간소화하고 액세스 추적을 강화합니다.
- IBM Tivoli Federated Identity Manager – 사용자 중심의 통합형 SSO를 제공하여 검증된 파트너 간의 안전한 정보 공유를 지원하고 애플리케이션 통합을 간소화합니다. 분산형 포털과 메인프레임 환경 전반에서 SOA 및 웹 서비스 배포를 위한 개방형 표준이 사용됩니다.
- Tivoli Security Policy Manager – 보안 정책 관리를 중앙화하고 애플리케이션, 데이터베이스, 포털 및 서비스에 대한 데이터 액세스를 세부적으로 제어합니다.
- QRadar Security Intelligence Platform – 로그, 위협, 취약성 및 리스크 관련 데이터를 수집, 저장, 분석하고 쿼리하는 통합 아키텍처를 제공하여 내부 위협을 차단하고 규정 준수 비용을 관리합니다.
- IBM Security zSecure suite – 메인프레임 환경에서 보안 규정 준수를 보장하고 보안 사고를 모니터링 및 감사하며, 일상적인 관리 작업을 자동화합니다.

#### IBM 보안 ID 및 액세스 보장

IBM은 사용자 라이프사이클의 전반에서 ID 관리를 능률화하고 액세스 정책을 적용할 수 있도록 번들 형태의 소프트웨어 솔루션을 제공합니다. 이 솔루션에는 로그를 관리하고 고급 권한 사용자를 모니터링하는 기능이 갖춰져 있어 내부 위협을 더 효과적으로 탐지하고 감사 기능을 개선하면서 규정 준수 이니셔티브를 실현할 수 있습니다.

IBM IAM 서비스는 ID 증명에서 사용자 프로비저닝 및 액세스 제어에 이르기까지 ID 관리의 모든 영역을 포괄하는 통합적인 포트폴리오입니다.

IBM IAM 거버넌스 솔루션은 핵심적인 비즈니스 및 보안 요구 사항을 해결하기 위한 종합적인 접근법을 채택하였으며, 다음을 지원합니다.

- 사용자 액세스 탐지, 문서화 및 분석
- 사용자 액세스 거버넌스 프로세스 확립
- 제한조건을 적용하여 비즈니스 충돌을 효과적으로 관리
- 제어 가능하고 중앙화된 방식으로 정책을 적용
- 워크플로우, 태스크 및 프로세스의 자동화 촉진
- 적절한 액세스를 보장하고 규정 준수를 지원할 수 있도록 모니터링, 보고 및 감사 수행

### 실질적인 혜택을 제공하는 IBM IAM 거버넌스 솔루션

IAM 거버넌스 솔루션은 정책 기반의 접근을 통해 가시성, 제어 및 자동화의 이점을 제공하며 비즈니스별 사용자 액세스 요구 사항을 더 효율적으로 해결합니다. 다음은 이와 같은 방식으로 IT 효율을 높이고, 보안을 확장하며, 리스크를 최소화하고, 규정 준수를 강화한 IBM 고객의 사례입니다.

#### 라틴아메리카의 한 은행

브라질의 한 은행은 수많은 지점과 1,000여 개의 판매 지점을 통해 10만 명 이상의 고객에게 급여 담보 대출 및 신용 솔루션을 제공합니다. 이 은행은 각종 보안 표준을 따르고 수십 개 애플리케이션의 로그온 절차를 지원해야 했으며, 직원들에게 적절하고 신속한 액세스를 보장하고 브라질 규제 기준을 준수하는 데 어려움을 겪고 있었습니다.

이 고객은 보안을 강화하고 정보 액세스 절차를 간소화하고자 IBM의 통합 ID 관리 및 SSO 솔루션을 구축했습니다.

이 솔루션은 사용자가 적합한 애플리케이션에 액세스할 수 있도록 하고 IT 자산에 대한 액세스를 간소화합니다. 이제 직원과 상담원은 은행 네트워크에 한 번만 로그인하면 허가된 모든 애플리케이션에 신속하게 액세스할 수 있습니다. 과거에는 한 고객의 대출 업무를 처리하기 위해 15개 ~ 30개의 각기 다른 애플리케이션에 로그인해야 했습니다. 직원이 퇴사하거나 상담원의 임무가 바뀔 경우에도 보안 팀이 몇 개의 키만 누르면 모든 시스템에서 액세스 권한을 즉시 디프로비저닝하고 은행의 데이터를 안전하게 지킬 수 있습니다.

이 은행은 연간 헬프데스크 운영 비용을 약 R\$32,000(US\$20,000) 절감했습니다. 최대 5일이 소요되었던 신규 사용자 프로비저닝 시간은 단 2시간으로, 4시간이 소요되었던 암호 초기화 시간은 단 몇 초로 단축했습니다. 필요에 따라 신속한 사용자 디프로비저닝이 가능하여 시스템 보안이 향상되었고, 보안 팀은 추가 인원 없이도 새로운 프로젝트를 지원할 수 있게 되었습니다.

#### 유럽의 한 도시

유구한 역사를 자랑하는 체코의 한 도시는 상업과 관광의 중심지로 도약했습니다. 도시의 성장에 따라 통합적인 IT 보안을 실현하려면 시스템에 대한 무단 액세스를 감시하고 차단하는 프로세스 등, 여러 프로세스를 중앙화하고 지능적으로 자동화할 필요가 있었습니다.

이 도시는 직위, 역할, 부서를 기준으로 직원 계정 액세스를 자동화하는 규칙 기반 ID 관리 시스템을 구현했습니다. 이 시스템에서는 자동화된 계정 조정 프로세스를 통해 사전 정의된 규칙에 부합하지 않는 계정을 탐지하고 이를 수정하거나 제거합니다. 폐쇄 루프형 조정 프로세스에서 "고아(orphan) 계정", 즉 오래된 계정을 찾아내고, 퇴사한 직원의 계정 액세스 권한을 자동으로 삭제합니다. 이제 이 도시는 계정 액세스가 필요한 직원에게 액세스 권한을 신속하고 효율적인 방식으로 제공할 수 있으며, IT 시스템의 보안도 보장할 수 있습니다.

IAM 솔루션으로 도시는 다음과 같은 혜택을 누리게 되었습니다.

- 신입 직원의 업무 활성화 속도가 100% 향상 - 신입 직원이 모든 시스템에 대한 액세스 권한을 받는 데 소요되는 시간을 며칠에서 몇 시간으로 단축함으로써 업무 생산성을 높였습니다.
- 관리 효율성 향상 및 비용 절감 - 상근 직원 1명이 모든 사용자 계정을 관리할 수 있게 되면서, 다른 IT 팀원들이 회사의 IT 환경을 발전시키고 확장하는 데 주력할 수 있게 되었습니다.
- 직원 퇴사 후 몇 시간 내에 해당 계정을 비활성화하고 고아 계정을 찾아내어 삭제함으로써 시스템 보안이 강화되었습니다.

#### 남아메리카의 한 사회복지기관

우루과이에서는 아기가 태어나면 병원에서 정부의 사회 보장 및 복지 기관에 온라인으로 통보되게 하는 중대한 파일럿 프로그램이 진행 중입니다. 이는 종이 문서 기반 프로세스를 대체하고 효율성과 투명성을 높이기 위한 우루과이 전자정부 프로그램의 일환입니다. 이 온라인 서비스는 약 5만 명의 공무원과 200만 명의 시민이 이용하게 됩니다.

이 기관은 IBM 및 IBM 비즈니스 파트너와 손잡고 멀티티어 아키텍처를 구현했습니다. 이 아키텍처는 전자정부 서비스를 위한 종합적인 보안 솔루션을 제공하고 전송 보안, 액세스 제어, ID 관리와 같은 문제를 해결합니다. IBM WebSphere® DataPower® Integration Appliance가 IBM Tivoli Security Policy Manager로부터 정책을 수신하는 정책 적용 지점의 역할을 하여 웹 서비스의 기밀성과 무결성을 유지합니다. Tivoli Federated Identity Manager는 메시지 전송을 요청한 사람의 ID를 확인하기 위한 보안 토큰을 발급합니다. IBM Tivoli Access Manager for e-business는 시민과 공무원이 빠르고 안전하게 온라인 서비스를 이용할 수 있도록 중앙화된 인증, 정책 관리 및 액세스 제어 서비스를 제공합니다. IBM Tivoli Directory Server와 IBM Tivoli Identity Manager는 신뢰할 수 있는 ID 데이터를 제공하여 모든 웹 서비스에서 인증 프로세스를 구현합니다.

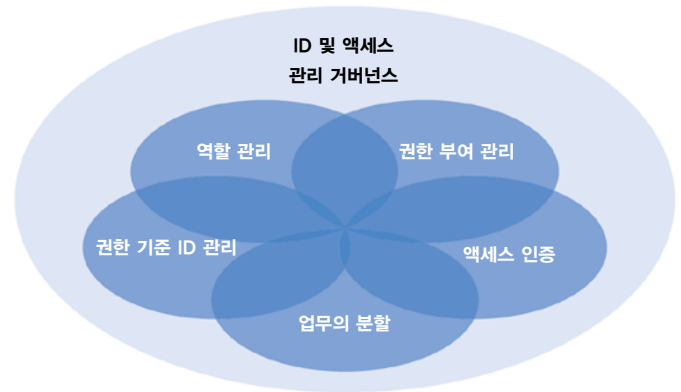


그림 4: 비즈니스 우선 순위에 따라 먼저 ID 관리의 하위 영역에서 시작한 다음, 전체 IAM 거버넌스를 위한 계획을 수립해야 합니다.

#### IAM 거버넌스를 통한 보안 및 비즈니스 효율성 향상

각종 규제와 관련된 문제가 늘어나고, 데이터의 양이 증가하고, 소셜 비즈니스로 인한 액세스 요구 사항이 계속해서 변화하면서, 기업의 일상적 보안 및 비즈니스 운영뿐 아니라 지속적인 규정 준수의 측면에서도 IAM 거버넌스 솔루션은 더욱 중요한 위치를 차지하게 되었습니다. IAM은 전략적인 정책 기반 접근을 통해 사용자가 변화에 대처하고, 관리 비용을 줄이고, 가장 중요한 정보 자산을 보호하도록 돕습니다.

여러 요인들을 고려할 때, IT의 주변 영역에 머물러 있었던 IAM이 IT의 중심으로 옮겨온 것은 당연한 흐름이라고 볼 수 있습니다. IBM IAM 거버넌스 솔루션은 고객이 다음과 같은 다양한 보안 및 비즈니스 중심의 혜택을 누릴 수 있도록 합니다.

- 중앙화된 뷰와 비즈니스 프로세스를 통해 ID를 확인하고 액세스 권한을 부여하면서 규정 준수를 강화합니다.

- 개별적인 ID 관리 솔루션을 통합 솔루션으로 대체함으로써 비용을 절감합니다.
- 직원 로그인 및 인증 정보의 수를 줄여 보안을 강화하고 비용을 절감합니다.
- SSO 환경과 온디맨드 액세스 프로비저닝을 통해 생산성을 높이고 헬프데스크 비용을 줄이면서 직원 및/또는 고객의 만족도를 높입니다.
- 시장 진출에 소요되는 시간을 단축하고 중앙화, 표준화된 보안 인프라를 갖추어 비즈니스 유연성을 높입니다.
- 중앙의 감사 뷰를 통해 런타임 승인 이벤트를 감시하여 악성 행위를 더 수월하게 탐지합니다.

### IBM을 선택해야 하는 이유

일관성 있는 IAM 거버넌스는 데이터 무결성을 보호하고, 규정을 준수할 수 있도록 지원합니다. IBM은 글로벌한 시각과 함께 각종 산업 분야에서 끊임없이 변화하고 있는 지역별 요구 사항에 대한 식견을 갖추고 있는 기업이며, 전 세계 IAM 시장에서 리더로 인정 받고 있습니다. IBM 솔루션의 우수성은 업계 전문가 및 보안 커뮤니티에 의해서도 지속적으로 입증되고 있습니다. 각종 분석 보고서에서 리더로 평가 받고 있으며, SC Computing 매거진에서는 2011년 최우수 ID 관리 솔루션(Best Identity Management solution)으로 선정되기도 했습니다. 상당수의 IAM 공급업체는 전체 IAM 거버넌스 솔루션의 범위 중 일부만 제공하며, 고객은 여러 공급업체의 제품을 각각 구축하고 관리해야 하는 부담을 안게 됩니다. 그러나 IBM의 포괄적인 통합형 IAM 소프트웨어 및 서비스 솔루션은 Oracle, Microsoft, SAP와 같은 타사 환경도 모두 지원합니다.

### 추가 정보

IBM 보안 시스템에 대한 자세한 정보는 IBM 영업 담당자 또는 IBM 비즈니스 파트너에게 문의하거나 [ibm.com/security](http://ibm.com/security)를 참조하십시오.

또한 IBM Global Financing의 금융 솔루션은 현금을 효과적으로 관리하고, 노후한 기술로부터 투자를 보호하며, 총소유비용과 ROI를 보다 향상시켜줍니다. 아울러, IBM의 Global Asset Recovery Services는 새롭고 보다 에너지 효율적인 솔루션을 통해 환경 문제에도 대응할 수 있도록 돕고 있습니다. IBM Global Financing에 대한 자세한 정보는 [ibm.com/financing](http://ibm.com/financing)에서 확인하실 수 있습니다.



© Copyright IBM Corporation 2012

IBM Corporation Software Group Route 100  
Somers, NY 10589  
U.S.A.

Produced in the United States of America  
January 2012

IBM, IBM 로고, ibm.com 및 X-Force는 미국 또는 기타 국가에서 사용되는 International Business Machines Corporation의 상표 또는 등록상표입니다. 이와 함께 기타 IBM 상표가 기재된 용어가 상표 기호(® 또는 ™)와 함께 이 정보에 처음 표시된 경우, 이와 같은 기호는 이 정보를 발행할 때 미국에서 IBM이 소유한 등록상표 또는 일반 법적 상표입니다. 또한 이러한 상표는 기타 국가에서 등록상표 또는 일반 법적 상표입니다. 현재 IBM 상표 목록은 웹 "저작권 및 상표 정보" ([www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml))에 있습니다. 기타 회사, 제품 또는 서비스 이름은 타사의 상표 또는 서비스표입니다.

본 문서는 발행일 기준으로 최신이고 IBM은 이를 통지없이 변경할 수 있습니다.

본 문서에서 언급된 모든 오퍼링이 IBM이 영업하고 있는 모든 국가에서 제공된다는 것을 의미하지는 않습니다.

제품 데이터의 정확성은 해당 데이터의 최초 공개일 현재로 이미 검토된 바 있습니다. 제품 데이터는 별도의 통지 없이 변경될 수 있습니다. IBM이 제시하는 장래 방향 및 계획에 대한 모든 진술은 특별한 통지없이 변경 또는 철회될 수 있으며 단지 목표 및 대상을 제시하는 것입니다.

법적 요구사항을 준수하는지 확인해야 할 책임은 IBM 고객에게 있습니다. 고객의 영업에 영향을 줄 수 있는 모든 관련 법률 및 규정과 이러한 법률을 준수하는 데 필요한 모든 조치를 식별하고 해석하기 위해 적절한 법률 고문의 자문을 구하는 것은 전적으로 고객의 책임입니다. IBM은 법률 자문을 제공하지 않으며 IBM의 서비스나 제품을 통해 관련 법률이나 규정에 대한 고객의 준수 여부가 확인된다고 진술하거나 보증하지 않습니다.



Please Recycle