RSA ARCHER® THIRD PARTY GOVERNANCE

소개

공급업체가 제공한 제품의 오류, 클라우드 서비스 운영 중단, 무차별적인 타사 공급업체 데이터 침해 등 타사 관계에 대한 부정적인 뉴스가 연일 헤드라인을 장식하고 있습니다. 타사 공급업체를 통해 제품 및 서비스를 제공하거나 강화하는 빈도가 늘어나고 있습니다. 그런데 이들 타사 공급업체에는 또 다른 타사가 서비스를 제공합니다.

비즈니스를 운영에 사용하는 타사 제품 및 서비스가 늘어날수록 위험 이벤트와 성능 저하의 빈도 및 영향도 증가합니다. 또한 이러한 위험의 수, 복잡성 및 속도가 빠르게 증가하고 있으며, 대부분의 조직은 적절한 직원과 가용 리소스를 갖추고 있지 않습니다. 공급업체 프로필, 업무 세부 정보 및 성능 데이터가 조직 내의 여러 팀에 흩어져 있는 경우가 많으며, 이 경우 타사 관계의 비즈니스 컨텍스트 및 중요도를 완벽하게 이해할 수 없습니다.

타사 위험 및 성능을 관리하는 일관된 전사적 프레임워크 없이는 전체 사업부와 관련된 타사 위험을 일관적으로 식별, 진단, 평가, 처리 및 모니터링하는 것이 불가능합니다. 결과적으로 타사 위험 및 성능에 대한 단일 정보 소스를 찾기가 어렵습니다.

타사 위험 및 성능 관리

타사 위험 및 성능 관리 프로세스를 전사적으로 표준화하면 공통의 언어, 평가 기준, 제어 및 프로세스를 설정하여 위험을 신속하게 이해하고 우선 순위에 따라 관리할 수 있습니다. 이와 같이 RSA Archer Third Party Governance를 사용하면 타사 위험을 정확하게 확인할 수 있으므로 타사 위험에 대한 정확한 정보를 경영진에 제공하여 리소스를 빠르게 할당하고 비즈니스 의사 결정을 개선할 수 있습니다.

RSA ARCHER THIRD PARTY GOVERNANCE의 이점

RSA Archer Third Party Governance는 공급업체 관계에 대한 감독을 자동화하고 간소화합니다. 이 솔루션을 사용하면 IRM(Integrated Risk Management) 프로그램의 일환으로 전체 타사 관리 수명주기 내내 규제 의무와 모범 사례를 이행하는 데 필요한 핵심 활동을 수행할 수 있습니다. 예정된 관계를 파악하고, 해당하는 이해 관계자와 연계하고, 계약상의 위험, 재정 건전성 및 여러 위험 범주별 기본 위험을 진단할 수 있습니다. 이를 통해 위험에 기반하여 타사를 선택하고, 성능 지표를 설정해 타사 수명주기 내내 프로그램을 모니터링하고 관리할 수 있습니다.

타사 관계에 대한 이해

조직에서 타사를 사용하는 사례가 늘어나면 조직이 사용하는 타사와 이러한 타사가 야기할 수 있는 위험을 카탈로그로 작성하고 진단할 수 있어야 합니다. 카탈로그 작성 및 진단은 타사 의존성 및 관련 위험을 이해하는 데 필수적인 작업이며, 타사 성과를 최적화하고 예상치 못한 사건과 손실을 방지하는 첫 단계입니다.

확실한 의사 결정과 조치

타사 위험에 대한 의사 결정이 조직의 위험 성향 및 허용도에 따라 일관적으로 내려지고 있는지, 적절한 위험 해결책이 구축되어 있는지 확인해야 합니다. 타사 위험을 최소화하려면 지속적으로 위험을 평가하고 조직의 위험 허용도에 따라 제어 수단 및 위험 전가 기술을 적용하는 관리자가 누구인지를 알고 있어야 합니다. 조직의 최전방에서 적절한 조치를 취할 책임은 이러한 관리자에게 있습니다.

타사 관계 모니터링

타사 리소스에 대한 의존도가 높아지면 신규 또는 업데이트된 공급업체 관계에 대한 최신 정보를 유지하고 기존 타사 관계에서 발생하는 중요한 변경 사항을 모니터링하는 것이 중요합니다. 변하지 않는 타사 관계는 없으며 위험은 계속해서 발생하고 진화합니다. 결국 타사 관계에 존재할 수 있는 중요한 위험을 확인하는 일은 조직의 몫입니다.

RSA ARCHER THIRD PARTY GOVERNANCE

RSA Archer Third Party Governance를 사용하면 예정된 관계를 파악하고, 해당하는 이해 관계자와 연계하고, 계약상의 위험, 재정 건전성 및 여러 위험 범주별 기본 위험을 진단할 수 있습니다. 이를 통해 위험에 기반하여 타사를 선택하고 성능 지표를 설정할 수 있습니다. RSA Archer Third Party Governance는 전체 타사 관리 수명주기 내내 규제 의무 및 모범 사례를 이행하는 데 필요한 주요 활동을 용이하게 하여 공급업체 관계에 대한 감독을 자동화하고 간소화합니다.

RSA Archer Third Party Governance는 타사 위험 및 성능 관리 프로그램의 완성도를 높이면서 고유한 비즈니스 요구 사항을 충족하는 여러 활용 사례를 제공합니다.

Third Party Catalog

RSA Archer Third Party Catalog는 모든 타사 관계, 업무 및 관련 계약과 조직에서 각 타사 관계를 책임지는 사업부 및 담당자 정보를 문서화하는 기능을 제공합니다. 또한 단일 저장소에 저장된 프로필, 업무 협약, 타사 비즈니스 계층, 계약, 설비, 타사 담당자 연락처를 비롯한 모든 타사 정보를 보고할 수 있습니다.

Third Party Security Risk Monitoring

RSA Archer Third Party Security Risk Monitoring은 투명한 보안 측정, 분석 및 분석가 수준의 통찰력을 제공하여 타사 위험 관리 프로그램의 성능을 대폭 향상시킵니다. 또한 타사 IT 위험 환경에 실행할 수 있는 인텔리전스를 제공합니다. AI(Artificial Intelligence)를 사용하여 각 공급업체의 IT 규모를 검색하고 분석하여 각 자산의 가치를 자동으로 측정할 수 있습니다.

Third Party Engagement

RSA Archer Third Party Engagement를 사용하면 타사로부터 받는 제품 및 서비스에 대한 정보를 더 완벽하게 문서화할 수 있어 내재된 위험 노출의 양을 명확하게 파악할 수 있습니다. 또한 제품 및 서비스 업무를 지원하는 비즈니스 프로세스에 연결하여 추가 관련자, 보험 증서 및 마스터 서비스 계약을 문서화할 수 있습니다. 이 정보는 타사에 대한 의존성을 포괄적으로 이해하는 데 도움이 됩니다. 또한 계약 검토, 계약상의 위험 진단 및 타사의 재정 건전성 진단 및 여러 위험 범주에 포함되는 기본적인 위험 진단을 수행할 수 있습니다.

Third Party Risk Management

RSA Archer Third Party Risk Management를 사용하면 조직에 제공하는 업무와 관련된 거버넌스 및 제어 수단이 타사에 갖춰져 있는지를 진단할 수 있습니다. 이러한 진단을 수행하면 재정 건전성, 계약상의 위험, 규정 준수/법적 분쟁, 신뢰성, 정보 보안, 평판, 회복탄력성, 전략, 지속 가능성, 추가 관련자 위험 등의 여러 위험 범주를 기준으로 타사 업무에서 발생할 수 있는 위험에 대한 점수를 산출할 수 있습니다. 구성 가능한 질의 응답서를 사용하여 관련된 지원 문서를 수집하고 추가 분석을 수행할 수 있습니다. 이러한 질의 응답서의 결과는 조직에 제공하는 모든 업무에 대한 타사의 전체 잔류 위험 프로필을 결정하는 요인으로 고려됩니다. 예외 및 문제 해결 계획을 설정하고 해결될 때까지 모니터링하는 동안 위험 진단 결과를 자동으로 파악하고 관리할 수 있습니다.

Third Party Governance

RSA Archer Third Party Governance를 사용하면 각 타사의 성능을 모니터링할 수 있습니다. 품질, 혁신, 성과 및 관계의 네 가지 범주로 각 업무에 대한 메트릭을 설정할 수 있습니다. 각 업무를 설명하는 지표를 타사에 반영하여 타사가 조직에 제공하는 업무 전반에 대한 성능을 파악할 수 있습니다.

결론

RSA Archer Third Party Governance는 타사 거버넌스 프로그램을 위한 집계, 시각화 및 관리 지점을 제공합니다. RSA Archer Third Party Governance는 타사 및 추가 관련자에 대한 위험 데이터를 분산된 위험 저장소에서 단일 위치로 통합하여, 전체 타사 수명주기에 대한 이해, 우선 순위 지정 및 관리를 개선하며, 위험 관리에 대한 책임 의식 및 문화를 강화하는 동시에 효율적으로 프로그램을 관리할 수 있습니다.

디지털 위험은 모두에게 중요한 과제이며
이 위험을 관리하도록 지원하는 것은 RSA의 몫입니다

RSA의 비즈니스 중심 보안 솔루션은 통합된 가시성, 자동화된 분석 정보 및 조율된 작업에 따라 디지털 위험을 관리하는 통합된 접근 방식을 조직에 제공합니다. RSA 솔루션은 지능형 공격을 효과적으로 탐지하고 대응하며, 사용자 액세스 제어를 관리하고, 비즈니스 위험, 부정 행위 및 사이버 범죄를 줄이도록 설계되었습니다. RSA는 전 세계 수백만 명의 사용자를 보호하고, Fortune지 선정 500대 기업의 90%가 넘는 기업이 성장하고 혁신 변화에 지속적으로 적응할 수 있도록 지원합니다.

역동적이고 위험도 높은 디지털 세상에서 성공하는 방법을 rsa.com/ko-kr에서 확인하십시오.