지침

사이버보안 상대방 리스크 평가

시작 안내

목차

자격 및 제한 조건

본 문서는 SWIFT 사용자가 금융 서비스 생태계 내에서 상대방의 사이버보안 데이터를 사용하고 해석하는 방법에 관한 일반적이면서 구속력이 없는 지침을 제공합니다. 본 문서는 거버넌스에 대한 바람직한 접근법과 사이버보안 리스크 데이터의 공유 및 기관의 기존 리스크 관리 프레임워크로의 통합 프로세스에 관한 제안사항을 제공합니다.

사용자별 특수한 문제점이나 요건은 다루지 않습니다.

본 문서에 들어있는 내용은 완전한 것이 아니며 건전한 판단이나 모범관행의 준수를 대체하는 것도 아닙니다.

사용자는 지침이나 추천사항의 결과로서 취한 일체의 조치 또는 내린 결정에 대하여, 그리고 본 문서에 포함된 데이터 일체의 해석에 대하여 단독으로 그리고 전적으로 책임집니다. SWIFT는 본 문서의 내용, 본 문서의 내용을 근거로 또는 그와 관련하여 취한 조치나 내린 결정 또는 그 결과에 대하여 어떠한 책임도 부인합니다. 본 문서에 있는 어느 내용도 SWIFT 측에 어떠한 의무, 진술 또는 보증을 구성하는 것으로 이해하거나 해석하면 안 됩니다.

SWIFT는 본 문서를 정보 목적으로만 제공합니다. 본 문서에 있는 정보는 시간이 지나면서 바뀔 수 있습니다. 사용자는 반드시 이용 가능한 최신판을 항상 참조하여야 합니다.

고객의 소리

귀사의 상대방에 적용되는 사이버 리스크 관리에서 직면하는 주요 난제는 무엇입니까?

"우리가 직면하는 주요 난제는 상대방에게 존재하는 사이버 통제에 접근하는 것입니다. 각 상대방의 통제 수준을 잘 모르기 때문에 사이버 리스크 관리가 어렵습니다. 약점이 하나만 있어도 전체 환경의 보안이 무너질 수 있습니다. 이것이 바로 상대방 사이버보안 실사 검토를 실시하는 것이 아주 중요한 이유입니다.

주요 문제를 보면 다음과 같습니다.

- 벤치마킹 목적으로 활용될 수 있는 모든 상대방이 사용하는 일관된 표준 찾기
- 상대방으로 하여금 그들의 보안 통제 또는 그 부족함에 대한 정보를 공유토록 하는 것
- 상대방이 제공한 정보의 정확성 검증
- 기업이 정보를 이해하고 동 정보를 근거로 적절한 사업 결정을 내릴 수 있도록 해당 기업에 소중한 리스크 정보를 제공할 수 있도록 데이터를 소비하고 처리하는 것
- 일체의 문제점을 사후관리하여 그러한 문제점을 치유하고 해결하며 그 사이에 보정 통제를 실시하는 데 합의하는 것"

요약

사이버 보안은 금융서비스 분야에 여전히 주요 위협 요소입니다. 본 지침은 은행업무 및 지급 생태계 내의 조직이 매일 거래하는 상대방이 부과하는 사이버보안 리스크를 어떻게 평가할 것인가에 대한 문제를 다룹니다.

본 지침은 각 기관이 해결하기 위해 살펴야 할 네 분야를 다룹니다. 즉, 거버넌스 모델 확립, 사이버보안 리스크 관리 프레임워크 수립, 사이버보안 리스크 조치 채택, 상대방의 사이버보안 '인증' 데이터 통합입니다.

상대방에 의하여 발생하는 것을 포함하여 사이버보안 리스크는 운영, 재무 및 규제 리스크와 같은 다른 유형의 리스크와 함께 관리되어야 합니다. 많은 기관이 사이버리스크 평가를 그들의 기존 상대방 리스크 프로세스에 통합하려 작업 중입니다.

이 프로세스에 대한 감독, 즉 **거버넌스**는 올바른 책임을 가진 올바른 사람들이 의사결정 능력을 갖고 그 프로세스가 강력하고 반복하여 일어나도록 할 권한을 가져야 합니다. 견고한 거버넌스가 마련되어야 기관은 사이버보안 리스크 **관리 프레임워크**를 실행할 수 있게 됩니다. 여기에는 다음과 같은 방법을 통한 상대방의 리스크 평가가 포함됩니다.

- 리스크에 기초한 결정을 지원하기 위하여 필요한 데이터 수집.
- 이러한 데이터를 처리하여 가중치가 부여되고 리스크에 기초한 평가로 변형시키는데, 이는 일반적으로 숫자 점수 또는 적-황-녹색의 지표로 표시됨.
- 리스크를 완화시키거나 '해결'하기 위한 적절한 조치 채택.

기관에는 다양한 리스크 성향이 있을 수 있지만, 사이버보안 리스크 완화 조치 사례에는 다음 사항이 포함될 수 있습니다.

- 상대방의 거래에 대하여 추가 수준의 정밀조사를 실시.
- 상대방과 수행하는 거래의 유형을 제한.
- 상대방에게 추가적인 통제나 사기 탐지 조치를 실행하도록 요구.
- 상대방에게 그들 정보를 독립적인 평가를 통해 입증하도록 요구.
- 상대방 합의서 및 계약서를 재평가.

이러한 거버넌스 모델 및 리스크 관리 내에서, 기관은 상대방의 사이버 준비상황에 대한 데이터 통합을 고려하여야 합니다.

SWIFT가 고객 보안 프로그램(Customer Security Programme, CSP)의 일환으로 도입한 고객 보안 통제 프레임워크 (Customer Security Controls Framework, CSCF)는 이점에 있어서 매우 소중합니다. CSCF는 SWIFT 사용자를 위한 일련의 의무적인 그리고 자문 차원의 보안 통제를 기술함으로써 전체 업계에 대한 보안 기초를 확립하였습니다. 모든 사용자들은 자신의 현지 SWIFT 인프라에 반드시 이를 구현하고 의무적인 보안 통제와 비교하면서 준수를 자체 인증하여야 합니다.

자체 인증이 발표되면 사용자는 이를 모든 자신의 상대방에게 알려서 개별적인 통제 준수를 입증하고, 상대방도 동등하게 서로에게 이를 요구할 수 있습니다. 사용자는 상대방별로 또는 일괄적으로 데이터를 열람하고 전송하여 데이터를 더 잘 '**소비하고**' 리스크 기반 의사결정 프레임워크에 통합할 수 있습니다.

CSCF는 업계의 투명성 및 표준화 향상에 도움을 줌으로써 조직이 사이버보안을 그들의 의사결정에 더 잘 통합할 수 있도록 해줍니다. 이러한 인증 데이터는 정보 면에서 풍부하여 SWIFT 사용자들에게는 유일한 사이버보안 리스크 데이터 소스입니다.

배경

사이버보안 및 사기는 여전히 최고의 전세계적인 위협입니다. 위협 행위자의 정교함은 증가하고 있으며, 대량 데이터 누출은 다반사가 되었고, 지능형 지속 위협 (Advance Persistent Threat, APT)을 통하여 거의 모든 사람이 목표가 될 수 있으며, '사물 인터넷' 유비쿼터스 '스마트' 장치가 디도스(DDoS) 무기로 사용될 수 있습니다.

금융업계 내에서 이러한 위협 행위자는 정교한 사이버보안 공격 위협을 가하고 있으며, 주된 목표는 **"자산 절도"** 입니다.

그러나 물론 은행업무 및 지급 생태계 내의 조직이 진공 상태에서 운영되는 것은 아닙니다. 그들은 매일 수많은 상대방과 상호작용하면서 거래합니다. 소수의 정교하면서도 자금력을 갖춘 위협 행위자로부터 SWIFT 고객에 대한 사이버공격이 계속되는 상황에서 리스크는 현실입니다. **조직은 사이버 공격에서 자신도 모르게 피해를 입은 희생자와 거래할 수 있는 잠재적 리스크를 어떻게 발견하고 대처해야 하는 것일까요?** 리스크를 관리하지 않고 자금을 잃어버린다면 금융 리스크가 심각해질 수 있습니다.

본 지침은 조직이 그들의 상대방이 부과하는 사이버보안 리스크에 대한 평가에 접근할 수 있는 방법을 살펴보고 네 가지의 주요 영역을 다룹니다.

- 사이버보안 리스크 관리를 위한 거버넌스 모델 수립.
- 사이버보안 리스크 관리 프레임워크 수립.
- 사이버보안 리스크 완화 조치 채택.
- SWIFT 상대방의 사이버보안 인증 데이터 통합.

본 문서의 나머지는 이러한 네 가지 주제를 논의하게 됩니다.

고객의 소리

사이버보안 인증 데이터가 이러한 하나 또는 일부 문제들을 해결하는 데 도움이 되었습니까? 그렇다면 어떻게 도움이 되었습니까?

"SWIFT의 고객 보안 인증 프로세스는 우리의 전체적인 회원 관리 프로그램을 보완하여 이러한 도전을 해결하는 데 도움이 되었습니다. 인증 데이터를 수령함으로써 이제는 상대방이 실시한 통제 수준을 이해할 수 있게 되었습니다. 각 상대방이 실시하는 통제의 유형 및 수준을 이해함으로써 사이버 리스크 관리를 더 잘 실시할 수 있게 되었습니다.

SWIFT CSP는 모든 상대방이 사용하는 일련의 대응조치를 지속적으로 제공하여 주기 때문에 벤치마킹에 활용할 수 있었습니다. 우리에게는 그것이 대학 입학팀의 SAT 시험입니다. 인증 도구는 상대방에 대한 접근권을 요청하고 부여하는 데 사용하기에 아주 쉽습니다. SWIFT CSP 프로그램은 상대방이 내부 및/또는 외부 감사에 의하여 검증된 답변을 얻는 수단을 제공함으로써 상대방의 답변에 대한 신뢰도 수준에서 도움을 줍니다. 우리는 인증 도구로부터의 데이터를 소비하여 보고서 및 차트를 만들 수 있는 계량 모델을 개발하였습니다."

사이버보안 리스크 관리를 위한 거버넌스 모델 수립

상대방에 의한 것을 포함하여 사이버보안 리스크는 운영, 재무 및 규제 리스크와 같은 다른 유형의 리스크와 함께 관리되어야 합니다.

이러한 리스크 관리 프로세스의 감독, 즉 거버넌스는 올바른 책임을 가진 올바른 사람들이 의사결정 능력을 가짐으로써 프로세스가 강력하고 반복적이며 예외를 관리할 수 있도록 만들어져야 합니다.

상급 위원회 구조

사이버보안 리스크 거버넌스는 전체론적 기능으로 고려되어야 합니다. 즉, IT 또는 업무 내의 고립된 후선업무 부서로 제한되기보다는 전체로서 사업을 책임지는 사람들이 중앙에서 감독하여야 합니다. 실제로, 상대방 리스크 관리는 리스크 위원회와 같이 자신의 권한과 충분한 자원을 보유한 **상급 위원회 조직**의 일부(또는 하부 조직)이 되어야 합니다.

이러한 여러 부서에 걸친 거버넌스 내에서, 책임을 '세(3) 방어선'에 조정하는 것도 고려하여야 합니다. 실제로 일상적인 운영 리스크 결정은 내부 통제 및 업무 절차를 집행할 책임이 있는 제1선(예: 사업, 업무, IT/사이버)이 담당하여야 한다는 것을 의미합니다. 예외 사항 및 상부 보고는 어느 정도 업무상 독립성이 있는 제2방어선(예: 컴플라이언스, 리스크)에서 관리하여야 합니다. 독립적인 제3방어선(예: 내부 감사)이 확실히 실행될 수 있도록 감독하여야 합니다.

사업 추진 이해관계자

거버넌스의 기능은 올바른 내부 이해관계자 그룹 전반에 대하여 영향력 있는 결정을 취할 권한을 보유한 적절한 직위의 개인이 수행하여야 합니다.

상대방 관리에 대한 일상적인 다수의 운영 리스크 결정을 오직 기술 또는 사이버보안담당 직원보다 **비즈니스 담당 직원**에 의하여 추진되어야 하는지는 논란이 있습니다. 하지만, 전반적인 거버넌스는 전체론적이고 다음과 같은 부문의 대표자들을 포함하여야 합니다.

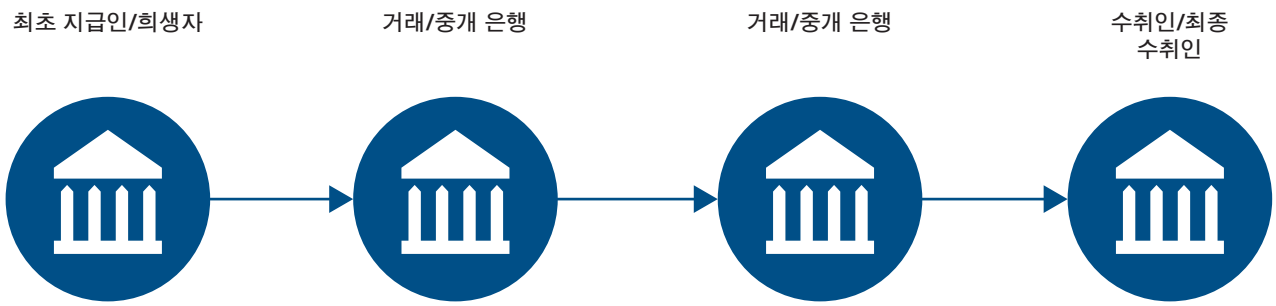
- **비즈니스** 및 상대방 관계 관리 대표자는 시장 및 상대방 익스포져를 평가하고 상대방과 연락을 위해 필요합니다.
- **지급 업무** 대표자는 업무 통제를 실시하고, 정상적인 처리 업무에서 제한사항을 조정하고 개입하기 위하여 필요합니다.
- **기술** 부문(예: IT, 정보보안, 사이버보안) 대표자는 추가적인 기술적 통제 또는 구체적인 사기 탐지 조치 실행을 요청하기 위하여 필요합니다.
- **리스크, 컴플라이언스 및 감사** 부문 대표자는 예외사항을 관리하고 독립적인 실사를 보장하기 위하여 필요합니다.

데이터의 민감성 및 보안 침해의 잠재적인 영향 때문에 이러한 프로세스에 대한 감독은 고위 임원이 담당하여야 하고, 해당 고위 임원은 리스크 평가와 상부 보고 프로세스를 추진하는 데 도움을 주고 그로 인한 조치 결정을 감독하여야 합니다.

명확한 권한

상대방 리스크 감독권을 가진 고위 위원회는 장기 전략뿐만 아니라 역할과 책임을 포함한 일상적인 운영 모델을 기술하는, 명확히 표현된 권한 또는 참조 조건을 마련하여야 합니다.
이러한 권한에는 또한 이사회 및 고위 경영진에게 상대방 리스크 현황, 구체적인 사건 및 진행상황, 그리고 동향에 대하여 정기적인 보고 필요성이 포함되어야 합니다.

사이버보안 상대방 리스크 평가 프레임워크



본 지침은 다음 기관을 대상으로 합니다.

- **중소기업**은 최초 지급인으로부터 지시서를 받습니다. 이러한 중소기업은 복수의 상대방 관계와 복잡한 내부 구조를 가질 수 있는 대형 기관에 비하여 제한된 수의 상대방을 가질 것입니다.
- **거래 은행**(규모와 무관)은 최초 지급인과 최종 수취인 사이의 거래 중개자 역할을 수행합니다.

고객의 소리

단순히 도구에서 자체 인증 데이터를 제출하는 것을 넘어서 사이버보안 인증 데이터를 사용하는 방법을 구체적으로 기술할 수 있습니까? 좀더 구체적으로 말하면, 이러한 인증 데이터를 귀사 상대방에 대한 보안 리스크 관리 맥락에서 어떻게 사용합니까?

"인증 도구는 일관성 있는 답변을 제공하므로 우리는 각 인증을 평가하고 답변에 근거한 숫자값을 적용할 수 있습니다. 이를 통하여 우리는 반복적인 정량적 및 정성적 조치를 각 인증에 적용할 수 있었습니다. 전에는 많은 경우에 일관성이 없는 설문지에만 의존하였습니다."

사이버보안 리스크 관리 프레임워크 수립

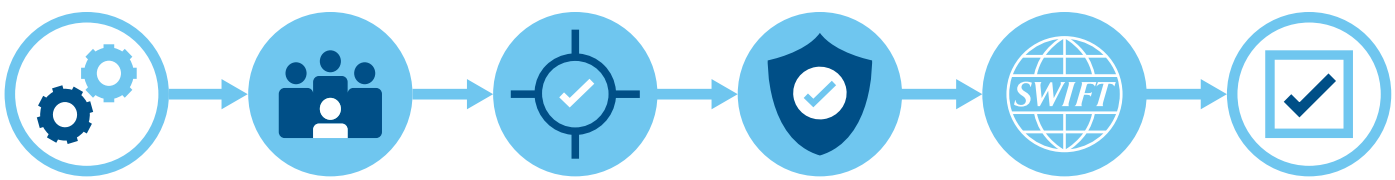
견고한 거버넌스를 마련한 기관은 일반적으로 리스크 관점에서 사이버보안에 접근하려 합니다. 즉, 그들은 리스크 수준을 평가하여 가장 필요한 곳에 예산을 투입하고 정해진 임계치 또는 관심 아래인 리스크는 수용합니다. 이러한 사이버보안 리스크 관리 프로세스 또는 프레임워크에는 몇 단계가 포함됩니다.

1. **필요한 상대방 리스크 데이터를 수집합니다.**

2. **데이터를 처리하여 리스크 수준을 평가합니다. 이는 일반적으로 종합 점수를 배정한 다음 회사의 리스크 성향 수준과 비교함으로써 이루어집니다.**

3. **리스크 점수를 기초로 해당 리스크를 관리 또는 "처리"하는 데 적합한 조치를 실행합니다.**

사이버보안 상대방 리스크 평가 프레임워크



사이버보안 리스크 관리를 위한 **거버넌스** 모델 수립

사이버보안 **리스크 관리** 프레임워크 수립

사이버보안 리스크 완화 **조치 채택**

SWIFT 상대방의 사이버보안 **인증 데이터** 통합

상대방 리스크 데이터

기관은 사이버보안 관점에서 상대방의 리스크 프로필을 알아보는 데 도움을 받기 위하여 다양한 데이터를 수집하여 처리합니다.

리스크 데이터는 광범위하게 세 범주로 분류됩니다. 상대방이 사업을 운영하는 외부 환경에 관련된 데이터, 상대방과의 사업 관계를 기술하는 데이터, 거래에 관한 데이터.

1. 상대방이 사업을 운영하는 외부 환경에 관련된 리스크

- **운영 국가/지역** - 상대방이 사업을 운영하는 관할권에서의 사이버보안, 규제 및 범죄/사기 수준에 대한 조치를 취할 수 있습니다. 이것은 바젤 AML 리스크 보고서와 같이 공개적으로 입수할 수 있는 자원을 이용하여 평가할 수 있습니다.
- **업계 유형** - 일부 부문은 다른 부문보다 더 자주 사이버보안 공격 및 데이터 침해를 당하므로 공격 가능성과 상관관계가 있을 수 있습니다.
- **상대방에 대한 규제 감독의 정도** 및 현지 감독기관이 사이버보안 규정 또는 정책을 부과하고 있는 정도.

2. 상대방과의 사업 관계에 관련된 리스크

- **상대방 관계의 심도/기간** - 비교적 새로운 관계는 오랜 관계, 심도있는 관계 및 신뢰할 만한 관계보다 더 높은 리스크가 존재할 가능성이 있음.
- **상대방의 규모/소유 구조** - 특히 글로벌하게 시스템적으로 중요한 은행(GSIB)과 같이 더 큰 그룹의 일부인 경우에는 위협과 싸울 예산, 숙련된 자원 및 도구 이용 가능성과 상관관계가 있을 수 있음.
- **알려진 사이버 및 보안 사건** 또는 기타 입수할 수 있는 뉴스, 정보 또는 실사 자료.
- **상대방에 대한 기존의 리스크 평가**(예: 운영, 재무 또는 규제).

3. 거래 관련 리스크

- **거래 유형** - 일정한 유형의 거래는 다른 거래보다 원래 더 취약하므로 상대방과 수행하는 거래의 유형을 제한함(예: 명세서에 근거한 지급).
- **거래 금액** - 신용 리스크 익스포져라 표기함.
- **거래 빈도** - 기간당 거래량이 많으면 많을수록 잠재적 공격 가능성이 큼.

이러한 상대방 데이터가 취합되면 리스크 평가 프로세스를 적용할 수 있습니다.

리스크 평가 프로세스

상대방 데이터가 취합되면 기관은 이러한 데이터를 처리하여 리스크 기반 평가로 변형시킵니다. 이러한 평가 방법론은 기관별로 다를 수 있지만 일반적으로 세 접근법 중 하나를 따릅니다.

- **전문가 기반** - 평가가 전문가의 판단 및 전문가에 의한 리스크의 정성적 가치평가에 의하여 주도되는 경우.
- **규칙 기반** - 평가가 상대방이 각 리스크 요인에 대하여 점수를 얻는 방법에 대한 간단한 규칙을 이용한 의사결정 분지도를 통하여 이루어지는 경우.
- **모델 기반** - 평가가 상대방이 각 가중치가 부여된 리스크 요인에 대하여 점수를 매기는 방법을 기초로 분석적으로 얻어지는 경우.

접근법에 상관없이 상대방은 보통 전체적인 점수가 주어지는데, 이러한 점수는 일반적으로 적색, 황색 또는 녹색 지표로 표시됩니다.

리스크 완화 조치는 내부 리스크 성향과 비교한 이 점수에 따라 달라집니다. 예를 들면, 낮은 또는 녹색 점수를 받은 상대방은 추가적인 정밀 심사가 필요하지 않은 것으로 분류될 수 있지만 높은 또는 적색 점수를 받은 상대방은 리스크 완화 조치가 필요하다고 선정될 수 있습니다.

사이버보안 리스크 완화 조치 채택

리스크 관리 프레임워크를 이용하여 기관은 상대방과 관련된 보안 리스크 정도를 평가하고 분류할 수 있습니다. 그런 다음 기관은 리스크를 수용할지 아니면 리스크 완화 조치를 고려할지 결정을 내릴 수 있습니다.

사이버보안 리스크 완화 조치에는 다음 내용이 포함될 수 있습니다.

1. 상대방과의 사업 관계에 관련된 조치

- 관계를 강화하고 전반적인 재확신을 제공하기 위하여 적극적으로 **고위 경영진에 보고**.
- 상대방이 내부 또는 제3자/외부의 독립적인 평가를 통하여 아니면 기술적인 설명 문서나 시험 결과를 제공함으로써 **자신의 정보를 입증**하도록 요청.
- 상대방에게 **추가 통제** 또는 **사기 탐지** 조치를 실행하도록 요청.
- 상대방의 리스크 제거 및 계약의 변경이나 해지 가능성을 포함하여 상대방과의 **합의서 또는 계약서**를 재평가.

2. 상대방과의 더 엄격한 거래 거버넌스에 관련된 조치

- **사전에 정의된 임계치**를 위반하는 거래의 검토를 위한 표시. 여기에는 거래 유형, 거래 금액, 거래 통화 또는 최종 수취인의 프로필이 포함될 수 있습니다.
- 표시된 모든 거래에 대하여, 상대방과의 거래에 대한 직접 육안에 의한 감독 및/또는 쌍방의 확인과 같은 **추가 정밀조사** 실시.

위에 열거된 조치는 완전한 것이 아니므로 기관은 리스크를 관리하는 데 도움이 되도록 다른 통제수단 및 도구를 배치할 수 있습니다.

더 높은 리스크를 가진 상대방에 대한 조치 적용

더 높은 리스크를 가진 상대방의 경우에, 기관은 위에 열거한 조치를 결합하여 적용하기를 원할 수 있습니다. 일반적으로 기관은 사전에 정의된 금액이나 수량 임계치에 대한 지급 지시에 대하여 추가적인 정밀 조사를 적용하고 모니터링하기를 원합니다. 기관은 임계치를 조정할 수 있어야 하며, 또한 경고 숫자의 증가에 대처할 수 있는 도구와 역량을 가져야 하고, 최신 상대방 연락 정보 획득과 같이 거래를 수작업으로 처리할 수 있는 추가적인 노력이 필요합니다.

정밀 조사를 늘려야 하는 상황이 반드시 영구적일 필요는 없습니다. 예를 들어 상대방이 추가 조치를 준수하기 때문에 '낮은' 리스크 범주로 재분류되면 임계치를 변경하거나 제거할 수 있습니다.

완화 조치 실행에 대한 결정을 넘어서는 경우 각 기관은 상대방과의 관계를 전면적으로 또는 부분적으로 변경, 중단 또는 종료할 책임을 단독으로 그리고 전속적으로 집니다.

사이버보안 리스크 관리 프로세스가 마련되고 나면, 거버넌스가 리스크 프로필이 변경되었는지 평가하기 위하여 상대방에 대한 정기적인 심사를 취할 때는 신중하여야 합니다.

고객의 소리

사이버보안 인증 데이터를 어떻게 사이버 리스크 관리에 입력하고, 이를 중심으로 조직된 거버넌스는 어떤 것입니까?

"주간 보고서가 다른 리스크 부서와 함께 당사의 최고 리스크 책임자에게 제공됩니다. 우리는 미결 요청 숫자와 부여된 인증 숫자를 비교하면서 추적합니다. 부여된 인증에 대해서는 각 인증에 리스크 점수를 매긴 다음 점수가 매겨진 각 인증을 정성적 프로필에 적용합니다. 당사의 리스크 부서는 프로필 결과를 그들의 규율에 포함시키기 시작했습니다."

부록 **A: SWIFT** 상대방의 인증 데이터 통합

2016년 5월에 출시된 SWIFT의 고객 보안 프로그램(CSP)은 모든 SWIFT 사용자가 그들의 현지 SWIFT 관련 인프라 보안을 강화하는 것을 지원합니다.

SWIFT 고객 보안 통제 정책(CSCP)은 사용자 인증 프로세스와 관련 원칙, 역할 및 책임을 정의합니다. 또한, SWIFT는 전체 사용자 커뮤니티를 위한 의무적인 그리고 조언 차원의 통제의 보안 기초를 확립한 고객 보안 통제 프레임워크(Customer Security Control Framework, CS CF)를 개발하였습니다.

CSCP 정책은 사용자들로 하여금 일련의 **의무적인 보안 통제**의 준수를 자체 인증하도록 요구하고 또한 그들이 일련의 조언 차원의 통제 준수에 대하여도 자체 인증하도록 권장합니다. 사용자들은 자신의 준수 수준을 인증하고, 그러한 **인증**은 SWIFT가 제공한 KYC-보안 인증(KYC-SA) 애플리케이션을 통하여 공표되고 관리됩니다.

KYC-SA 도구에서 이용 가능한 주요 기능은 상호 합의 하에 기관이 **접근권 '요청' 및 '부여'**를 통하여 인증 데이터를 그들의 상대방과 교환할 수 있다는 점입니다. 그렇게 함으로써 기관은 상대방 리스크를 평가한 다음 인증된 컴플라이언스 수준을 기초로 상대방 리스크에 대한 결정을 할 수 있게 됩니다. 이러한 인증 데이터는 정보 면에서 풍부하고 유일한 사이버 보안 상대방 리스크 데이터입니다.

기관이 CSP 인증 데이터를 상대방 리스크 프레임워크에 통합하기 시작할 때 많은 요인을 고려하여야 합니다.

- 거버넌스 모델 고려사항.
- 리스크 관리 프레임워크 고려사항.
- 완화 조치에 대한 향후의 옵션.

이러한 세 고려 분야는 KYC-SA 도구의 전반적인 맥락 내에서 아래에 논의됩니다. 인증하는 사용자는 사용자 인증의 정확성에 대하여 책임을 지며 SWIFT는 이를 검증하지 않는다는 점을 강조하는 것이 중요합니다. CSP는 공유되어 SWIFT 사용자가 사용할 수 있는 보안 정보에서 일정한 수준의 **표준화** 및 **투명성**을 이룰 수 있도록 설계되었습니다.

부록 B에는 CSCF 프레임워크 및 CSCP 정책 문서로의 링크가 포함되어 있습니다.

또한, 부록 B에는 인증 데이터에 대한 접근권 요청/부여 방법과 인증 데이터를 엑셀 파일로 전송하는 방법에 관한 단계별 세부사항이 담긴 KYC-SA 사용자 지침으로의 링크도 포함되어 있습니다. 인증 데이터는 조직의 보안 책임자가 상대방별로 또는 모든 관련된 상대방 전부에 대하여 일괄적으로 전송할 수 있습니다. 하지만 이러한 지침은 거버넌스 배정, 데이터 처리, 리스크 평가 및 조치 할당과 같이 조직이 데이트를 소비하는 방법에 관해서는 기술하지 않습니다. 본 지침은 아래에 개괄적으로 기술되어 있습니다.

고객의 소리

상대방에게 귀사의 인증 데이터에 대해 접근권을 부여하는 거버넌스는 무엇입니까? 이 부분에 대한 책임이 나누어져 있습니까 (예: 리스크, 컴플라이언스, 법무 등)?

"상대방에게 인증 데이터에 대한 접근권을 부여하는 거버넌스 프로세스는 여러 팀이 참여하여야 합니다. 인증 데이터에 접근권을 부여하는 데 있어 투명성을 확보하기 위해서입니다. 내부 워크플로우 승인 프로세스가 있습니다. 내부적으로 승인되면, 관리팀이 인증 도구를 통해 접근권을 부여합니다."

거버넌스 모델 고려사항

인증 데이터 공유를 결정하거나 다른 기관에 그들의 데이터를 공유하도록 요청하기 전에 상대방 인증 데이터를 소비하는 전반적인 프로세스를 정해야 합니다. 특히 여기에는 공유를 어떻게 할 것인지, 그리고 누가 어떤 역할을 수행할 것인지가 포함되어야 합니다.

SWIFT가 기술적인 플랫폼을 제공하기는 하지만 기관의 거버넌스 모델 역시 상대방 보안 인증 데이터의 평가를 지원할 수 있도록 조정되어야 합니다. 인증 데이터에 대한 접근권을 '부여'하거나 '요청'할 때 광범위한 기관의 적절한 대표자를 고려해야 합니다. 그리고 데이터를 해당 기관의 기존 상대방 리스크 관리 프레임워크 내에서의 추가 요소로 보아야 합니다.

상대방에 접근권 부여(또는 거절)

요청하는 상대방에게 접근권을 부여하려면 거버넌스 모델은 '예' 또는 '아니오' 승인 결정 프로세스를 관리하는 사업 소유자를 명확히 지정하여야 합니다. 명확한 '부여권자'가 없으면 들어오는 인증 요청은 답을 하지 않은 채 남아있게 됩니다.

들어오는 요청을 부여하기 위하여 사용되는 승인 결정 기준은 일반적으로 리스크 위원회와 같은 고위 위원회, 또는 CISO, 법률고문 또는 최고 준법책임자와 같은 임원진이 서명하여야 합니다.

상대방에 접근권을 부여하는 데 있어 '부여자'가 사용하는 결정 기준 사례

- 인증 데이터를 지리적인 위치와 상관없이 글로벌 거래 은행과 공유함.
- 인증 데이터를 동일한 규제기관의 감독을 받는 동일한 지역에 있는 상대방과 공유함.
- 인증 데이터를 당사가 외부 평가 또는 감사를 통해 지원받는 '인증 유형'으로 보고할 수 있게 되면 공유함.
- 인증 데이터를 활발하게 메시지를 주고받는 모든 요청 상대방과 공유함.
- 인증 데이터를 우리 기관과 그들의 인증 데이터 역시 공유하는 요청 상대방과 공유함.
- 인증 데이터를 모든 요청 상대방과 공유함.

고위 위원회 조직이나 임원진이 결정 기준에 서명하여야 합니다. 이것이 이루어지고 나면 중간 관리자는 이러한 기준을 들어오는 요청에 적용하고 기술적 운영자에게 접근권을 부여 또는 거절하는 결정을 줍니다.

예외는 고위 위원회 조직이나 임원진에 보고되어야 합니다.

운영 차원에서 운영자(또는 "부여자")는 수령한 요청 및 취한 조치에 대한 요약 보고서를 규칙적으로(예: 주간 단위로) 경영진에 제출하여야 합니다.

접근권 부여 프로세스 플로우 예

1. '부여자' 역할을 운영자에게 배정.
2. 운영자는 상대방으로부터 접근권 요청을 수령함.
3. 운영자는 요청을 승인 기준과 비교 검토한 다음 긍정적이거나 부정적인 답변을 추천.
4. 중간 관리자는 추천을 검토하고 실행 허가를 주거나 대체 결정을 내리거나 임원진에 보고.
5. 운영자는 상대방 요청을 '수락'하거나 '거절'. 접근권을 거절하는 경우에 운영자는 거절 사유를 제공하여야 합니다. 여기에는 상대방과의 관계가 없거나 이 시점에서 인증 데이터를 공유할 준비가 되어 있지 않다는 사실도 포함될 수 있습니다.
6. 운영자는 규칙적으로(예: 주간 단위) 요청 상황 및 조치에 대한 요약 보고서를 제출합니다.

인증 도구는 또한 임원진이 규정한 기준을 충족하는 상대방 BIC의 '화이트리스트'를 만들 수 있도록 해줍니다. 이와 같이 하면 요청하는 즉시 그러한 상대방에 접근권을 자동적으로 부여할 수 있어 수작업 검토 및 승인 플로우를 피할 수 있습니다. 이러한 기능은 "자동 부여"라고 알려져 있습니다.

상대방의 접근권 요청

고위 위원회 조직이나 임원진은 상대방에게 접근권을 부여하는 기준에 서명하여야 합니다. 상대방 인증 데이터 요청 기준은 유사한 수준에서 결정되어야 합니다.

상대방 데이터에 대한 접근권 요청시 '요청자'가 사용하는 결정 기준 예

- 모든 상대방에 대하여 인증 데이터를 요청함
- 규칙적으로 상호작용을 하지 않은 상대방으로부터만 인증 데이터를 요청함
- 높은 리스크 지역에 소재하는 상대방으로부터만 인증 데이터를 요청함
- 이미 높은 리스크로 간주된 상대방으로부터만 인증 데이터를 요청함

결정 기준을 임원진이 규정하고 나면 인증 요청은 운영자("요청자")가 인증 도구에서 실행할 수 있습니다.

상대방 인증 데이터 접근권 요청 상황은 상대방에 대한 접근권 부여 상황 보고와 유사하게 규칙적으로(예: 주간 단위로) 경영진에 보고하여야 합니다.

접근권 요청 프로세스 플로우 예

1. '요청자' 역할을 운영자에게 배정
2. 임원진이 상대방 인증 데이터 접근권 요청에 대한 결정 기준을 규정
3. 운영자는 요청을 인증 도구를 통하여 상대방에게 발송
4. 상대방은 접근 요청을 '허락'하거나 '거절' 요청이 거절된 경우 임원진은 상대방과의 추가 관계를 고려하고 거절 사유가 완화된 후 접근권을 다시 요청하여야 함
5. 운영자는 규칙적으로(예: 주간 단위) 요청 상황 및 조치에 대한 요약 보고서를 제출

고객의 소리

상대방의 인증 데이터에 대한 접근권이 부여된 경우, 심각한 사이버보안 결정을 하도록 발단이 되는 정보를 받은 경우가 있습니까? 그렇다면, 상세히 설명해줄 수 있습니까?

"상대방 인증 데이터에 대한 접근권이 부여되고 나면 우리는 통제에 대한 대응책을 검토합니다. 그러나 아직 상대방의 인증을 기초로 사이버보안 결정을 한 적이 없습니다. 상대방 대응이 사이버 감염에 관한 우리의 내부 대화를 주도하였습니다."

리스크 관리 프레임워크 고려사항

상대방의 인증 데이터에 대한 접근권이 부여된 조직은 도구를 사용하여 데이터를 '소비'할 수 있습니다. 통제별 준수 수준을 포함하고 있는 이 인증 데이터는 상대방이 부과하는 리스크를 관리하는 데 도움이 되도록 조직의 리스크 기반 의사결정 프레임워크에 통합되어야 합니다.

사이버보안 인증 데이터를 자신의 기존 리스크 관리 프로세스에 포함시키기를 원하는 기관은 그 정보에 기초한 가중치와 점수를 적용하기를 원할 수 있습니다.

의미있는 가중치와 점수를 배정하는 것은 자세한 연습으로서, 기관은 이를 위하여 정보 보안, 업무, 기술, 리스크, 컴플라이언스, 비지니스 및 법무 부서와 같이 내부 이해관계자들 사이에 협업을 확보하여야 합니다.

가중치와 점수에 대한 모범적 접근법

- 상대방이 인증하지 않은 경우에 상대방에 점수를 매깁니다
- 상대방이 KYC-SA 접근권 요청에 응답하지 않는 경우 상대방에 점수를 매깁니다
- 지침에 따른 준수, 대체 수단에 의한 준수, 준수 부족, 또는 주어진 날짜까지의 향후 준수와 같이 각 CSCF 통제에 대한 준수 수준에 점수를 매깁니다
- 의무적이든 조언 차원이든, 각각의 특정한 통제에 상이한 가중치를 배정할 수 있습니다
- 기타 인증 변수에 다음과 같은 특정한 가중치를 부여할 수 있습니다.
  - **인프라 유형**
  - **인프라 구성요소** - 상대방이 인증을 받은 인터페이스를 사용하고 있는가?
  - **서비스 제공업체** - 상대방이 서비스 제공업체를 통하여 연결되는가? 그리고 그 제공업체의 인증 또는 준수 상태는 어떠한가?
  - **평가 유형** - 상대방은 조언을 얻기 위해 내부 또는 외부의 제3자를 고용하였는가? 아니면 그들의 인증이 내부 또는 외부의 독립된 평가에 의하여 입증되었는가? 아래를 보십시오

'평가 유형' 해석

자체 인증에 있어서 이 분야는 상대방이 그들의 인증된 준수 수준을 입증하기 위하여 독립적인 검토자를 이용한 정도를 파악하는 것입니다.

– **제3자의 독립적인 평가(외부 감사인에 의한 감사를 포함할 수 있음)** - 기관은 독립적인 외부 평가자를 이용하여 통제 준수를 검증합니다. 그 이름은 반드시 인증 기관이 선언하여야 합니다. – **내부의 독립적인 평가(내부 감사를 포함할 수 있음)** - 기관은 내부 평가 부서를 이용하여 통제 준수를 검증합니다.	각 통제에 배정된 준수 상황이 독립적으로 검증되었음을 더 합리적으로 보장할 수 있습니다. 이 수준의 보장을 할 수 있는 상대방은 더 신뢰할 수 있다는 것을 의미할 수 있습니다. 외부 평가자의 이름을 정밀 조사할 수 있습니다.
– **외부 회사에 의한 조언 차원의 검토** - 기관은 제3자를 고용하여 준수 평가에서 조언 서비스를 받을 수 있습니다. 그러한 제3자의 이름은 반드시 인증 기관이 공표하여야 합니다. – **내부의 독립적인 팀에 의한 조언 차원의 검토** - 기관은 독립적인 내부 당사자를 고용하여 준수 평가에 조언 서비스를 받습니다.	열거한 통제 상태에 대한 독립적인 검증에 어느 정도의 신뢰감을 줄 수 있습니다. 조언 차원의 평가는 고정된, 사전에 정의된 프레임워크에서 실시되지 않습니다. 완전한 평가 보고서를 약속하고 이용할 수 있으면 신뢰감이 더 높아질 수 있습니다. 표적 평가 또는 샘플 확인으로 보완될 수 있습니다.
– **자체 평가** - 기관은 정보를 자체 평가합니다(예: CISO, CRO 또는 다른 임원들의 서명).	상대방이 CSCF 통제 준수를 철저히 평가하였다는 최소한의 신뢰를 줄 수 있습니다.

추가 리스크 완화 조치

섹션 4에서 개괄적으로 기술한 일반적인 조치 외에 아래에 기술하는 바와 같이 SWIFT 사용에 특수한 많은 추가 옵션을 포함시키는 것을 고려할 수 있습니다.

조언 차원의 통제에 대한 준수 요청

일련의 의무적인 통제에 대한 기존의 자체 인증 의무 외에 기관은 일부 상대방 역시 조언 차원의 통제의 일부 또는 전부에 대하여 자체 인증하도록 요청하기를 원할 수 있습니다.

상대방의 사기 탐지 조치 활용

SWIFT 사용자는 일부 상대방이 정상적인 행동 양식을 나타내지 않는 변칙 또는 이상치를 찾는 사기 탐지 역량을 실행할 것을 요청하고자 할 수 있습니다. 이는 현재는 CSCF v2019에 조언 차원의 통제로 규정되어 있습니다.

예: SWIFT 일일 검증 보고서(DVR)

CSP 프로그램의 일환으로 SWIFT는 거래 양식 탐지 도구를 추가함으로써 금융범죄 준수 포트폴리오를 확대하였습니다. 이는 지급 사기와 관련된 리스크를 완화하기 위한 것입니다.

일일 검증 보고서(DVR)는 기관이 지급 거래 활동을 검증하고, 잠재적 리스크를 강조하고, 사기 사건이 발생하는 경우 빠르게 대응하는 것을 용이하게 합니다.

DVR은 전날의 지급 활동에 대한 정보를 제공합니다. 매일의 거래금액 및 거래량 총계를 이전의 24개월에 걸친 사용자의 일일 금액 및 거래량 평균과 비교함으로써 활동상의 중요한 변화를 빨리 확인하고 이해할 수 있도록 해줍니다.

취급하는 주요 두 영역은 다음과 같습니다.

- 활동 보고서를 통해 사용자는 일일 활동의 총계를 볼 수 있습니다. 일일 활동 총계는 메시지 유형, 통화, 국가 및 상대방별로 보여집니다. 일일 금액 및 거래량 총계뿐만 아니라 가장 큰 거래의 세부사항도 제공됩니다.
- 리스크 보고는 사기 리스크를 나타낼 수도 있는 대규모 또는 특이한 메시지 흐름을 강조하기 위한 것입니다. 동 보고서는 사용자가 타발 및 당발 지급 상대방과의 최대 규모의 단일 거래 및 최대 규모의 거래 흐름 총계를 선정하는 데 도움을 줍니다. 이전의 평균 매일 금액 및 거래량과의 비교를 통해 사용자는 활동의 변화를 평가할 수 있게 됩니다. 리스크 보고는 또한 당일 거래로부터 새로운 직접적인 그리고 간접적인 상대방의 결합도 강조합니다.

정보는 다음과 같은 주요 SWIFT 메시지 유형에 대하여 집계됩니다. MT 103, MT 202, MT 202COV, MT 205 및 MT 205COV.
DVR은 2016년에 시작되었습니다.

예: SWIFT 지급 통제 서비스(PCS)

지급 통제 서비스(Payment Controls Service, PCS)는 특별히 SWIFT 사용자가 기내 변칙 활동을 탐지하는 데 주로 도움을 줍니다. PCS는 상대방 정책에서 벗어나거나 평소답지 않아 사기 리스크가 있는 기내 지급을 실시간으로 탐지합니다. 이는 대역 외, 즉 사용자 구내를 벗어나 수행됩니다. 이는 기관은 위태롭다 하더라도 데이터는 신뢰할만하다는 것을 의미합니다.

PCS는 구독자가 정의한 정책 규칙을 사용하여 두 실시간 운영 모델 중 하나로 작동됩니다.

- 메시지 사본 및 경고, 또는
- 메시지 보류 및 경고

핵심은 PCS가 사용자로 하여금 많은 수의 파라미터에서 정책 규칙 환경을 설정할 수 있도록 해준다는 점입니다.

- 업무 달력, 비영업일 및 정상 영업 시간
- 통화 화이트리스트/블랙리스트, 단일 및 총계 지급 한도
- 국가 화이트리스트/블랙리스트, 단일 및 총계 지급 한도
- 국가, 통화, 단일 조직 또는 그룹 결합체에 대한 임계치
- 신규 기관: 과거 메시지 흐름을 기초로 신규 참가자 또는 체인과의 지급 확인
- 의심스러운 계좌: 고위험이라고 생각되는 계좌번호의 기관 블랙리스트와 최종 고객 계좌번호를 검증

PCS는 2018년 10월에 시작되었습니다.

기관이 수신인 사기 통제를 실시하기 전에 또는 기관이 상대방에게 발신인 사기 통제를 실시하도록 요청하기 전에 약관 및 기타 법률적인 고려사항을 검토하여야 한다는 점에 유의하십시오.

RMA로 관계를 세밀히 규정하고 이를 실시함

몇 년 전에 이루어진 관계는 시간이 지나면서 변화되었을 수도 있고 현재의 사업 양식과 맞지 않을 수도 있습니다. SWIFT 사용자는 관계 관리 애플리케이션(Relationship Management Application, RMA)으로 메시지를 발송하는 사람을 통제할 수 있는 것 외에도 RMA+로 메시지 유형을 제약할 수 있습니다. 예를 들면, 사용자는 자금 또는 거래 메시지는 수신하지만, 지급 메시지는 수신하지 않기로 합의할 수 있습니다.

예: SWIFT RMA 및 RMA Plus

관계 관리 애플리케이션(RMA)은 두 금융기관 사이의 키 교환 및 권한부여 프로세스로서 기관으로 하여금 어떤 상대방 기관이 자신에게 FIN 메시지를 보낼 수 있는지 정의할 수 있도록 합니다. 원하지 않는 모든 트래픽은 발신인 차원에서 차단되어 원하지 않는 메시지를 처리하는 것과 관련된 운영 리스크를 줄여줍니다.

RMA의 더욱 세련된 버전인 RMA Plus는 한 걸음 더 나아가 기관이 그들이 발신하기를 원하고 각 상대방으로부터 수신하기를 원하는 메시지 유형을 특정할 수 있도록 해줍니다. 예를 들면, 기관은 특정한 거래은행으로부터 신용장만을 수신하기를 원할 수 있습니다.

기관은 자신의 상대방으로부터 메시지를 받으려면 RMA 또는 RMA Plus 권한을 그러한 상대방에게 부여하여야 하며, RMA 기능은 Alliance Access 및 Alliance Entry SWIFT 인터페이스에 구축되어 있습니다.

시간이 지나면서 많은 기관이 많은 상대방 기관과 RMA 관계를 많이 개설하였습니다. 하지만 업무 관계가 바뀌거나 종료될 때 RMA 권한 목록이 항상 업데이트되는 것은 아닙니다. 그러므로 해당 기관은 비활성화된 RMA를 많이 가지고 있을 수 있으며 이를 모를 수도 있습니다.

휴면 또는 비활성화된 RMA를 정리하고 철회함으로써 기관은 그러한 활동에 관련된 시간과 비용을 최소화하고 리스크를 줄일 수 있습니다.

기관은 이런 정리 작업을 스스로 할 수 있습니다. 대안으로서 SWIFT는 RMA 및 RMA Plus 권한부여 '말소' 서비스를 제공합니다.

RMA는 2009년에 시작되었습니다.

부록 **B:** 용어집

용어	축약어	설명
SWIFT Customer Security Programme(SWIFT 고객 보안 프로그램)	CSP	**추가 정보는 여기를 클릭하십시오**
Customer Security Control Framework(고객 보안 통제 프레임워크)	CSCF	**추가 정보는 여기를 클릭하십시오**
Customer Security Control Policy(고객 보안 통제 정책)	CSCP	**추가 정보는 여기를 클릭하십시오**
Know Your Customer – Security Attestation (application) (고객 알기 - 보안 인증(애플리케이션))	KYC-SA	기초: **추가 정보는 여기를 클릭하십시오** 사용자 가이드: **추가 정보는 여기를 클릭하십시오**
Relationship Management Application(관계 관리 애플리케이션)	RMA	**추가 정보는 여기를 클릭하십시오**
Daily Validation Report(일일 검증 보고서)	DVR	**추가 정보는 여기를 클릭하십시오**
Payment Controls Service(지급 통제 서비스)	PCS	**추가 정보는 여기를 클릭하십시오**
Shared Infrastructure Provider(공유 인프라 제공자)	SIP	**추가 정보는 여기를 클릭하십시오**
Business Identifier Code(기관 식별자 코드)	BIC	**추가 정보는 여기를 클릭하십시오**
Chief Information Security Officer(최고 정보보안 책임자)	CISO	회사에서 정보 보안을 책임지는 가장 고위 임원을 지칭하는 일반적인 명칭

SWIFT 소개

SWIFT는 세계적인 회원 소유 협동조합으로서 안전한 금융 메시지 서비스를 제공하는 세계 최고의 선도자입니다. 당사는 커뮤니티에 메시지 플랫폼과 커뮤니케이션 표준을 제공하고 접근 및 통합, 확인, 분석 및 금융 범죄 컴플라이언스를 용이하게 하는 상품 및 서비스를 제공합니다.

당사의 메시지 플랫폼, 상품 및 서비스는 200개 이상의 국가와 지역에서 11,000개 이상의 은행 및 증권 조직, 시장 인프라 및 기업 고객을 연결하여 신뢰할 수 있는 방법으로 표준화된 금융 메시지를 안전하게 연락하고 교환할 수 있도록 합니다.

신뢰받는 제공자로서 당사는 글로벌 및 현지의 금융 흐름을 촉진하고, 전세계에서 무역 및 상거래를 지원합니다. 또한 운영상의 우수성을 과감히 추구하고 비용을 낮추고, 리스크를 줄이고, 업무상의 비효율성을 제거하는 방법을 지속적으로 모색합니다.

벨기에에 본사를 둔 SWIFT의 국제 거버넌스 및 감독 부문은 협동조합 구조의 중립적이며 글로벌한 성격을 강화하고 있습니다. SWIFT의 글로벌 사무소 네트워크는 모든 주요 금융 센터에서 진출하여 활동 중입니다.

이에 대한 추가 정보는 www.swift.com을 방문하거나 어카운트 매니저에 연락하거나 weareswift@swift.com으로 이메일을 보내주십시오.

57386 — 2019년 1월