삼정 KPMG

Strictly Confidential

암호화폐 거래소 AML 체계 구축을 위한 과제 및 업계 공통 기준의 필요성

Nov, 2019

KPMG Samjong Accounting Corp. / Governance Risk & Compliance Services

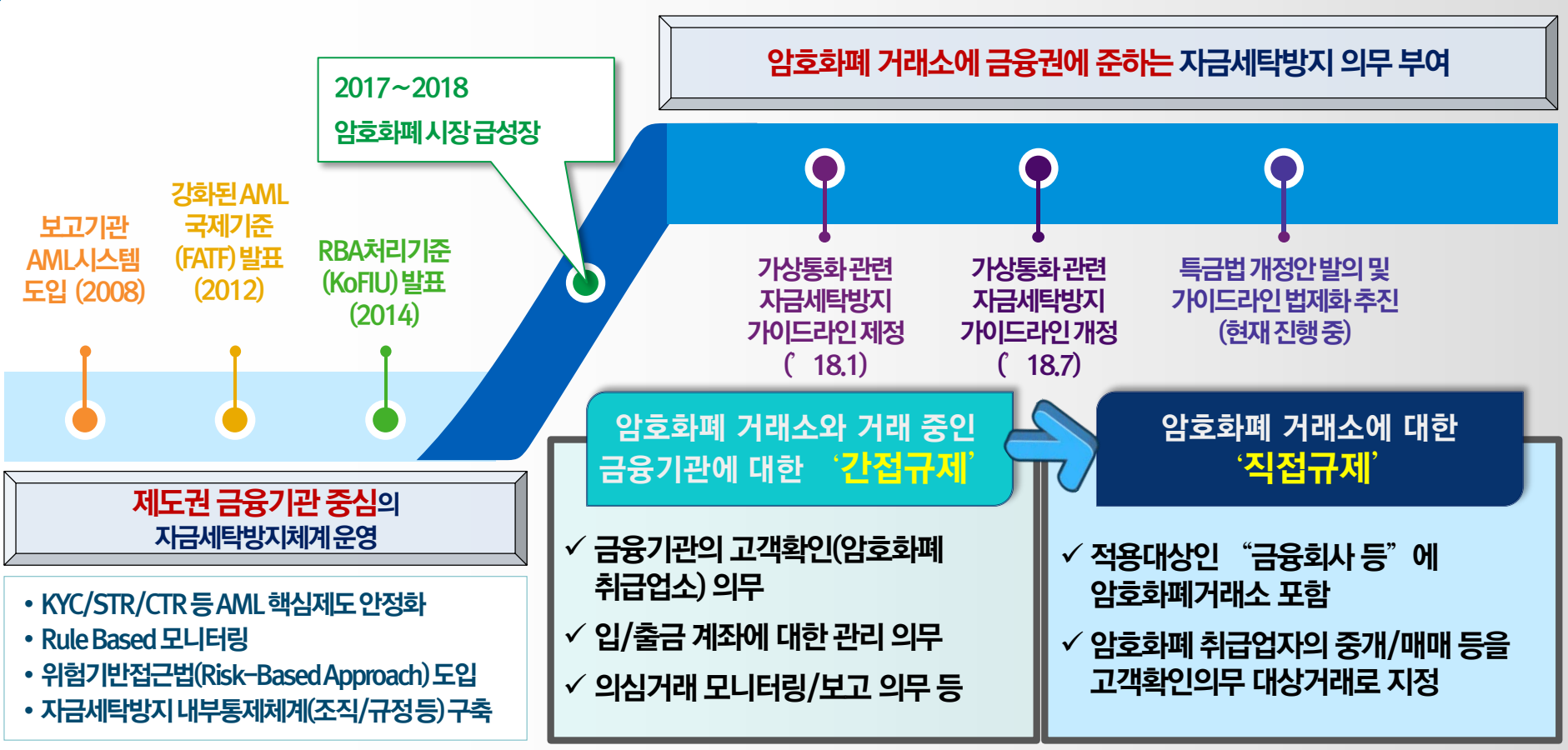
Contents

coindesk

Contents

1. 규제 요구사항의 이해 – 국내

최근 국내 암호화폐 관련 자금세탁방지 규제는 금융기관을 통한 간접규제에서 암호화폐 거래소에 대한 직접규제로 변화되는 양상을 보이고 있어, 보다 적극적인 대응이 필요합니다.



"암호화폐 거래소에 대한 **제도권 거래기관 편입** 및 **직접 규제 강화** 예정"

coindesk

삼정 KPMG

1. 규제 요구사항의 이해 – FATF Guidance

지난 6월 발표된 국제자금세탁방지기구(FATF) 권고안에 따라 암호화폐 거래소를 포함한 가상자산 서비스 제공업자의 자금세탁방지 체계 도입에 대한 국제 규제 요건이 강화되었습니다.

거래소 적용필요사항

- 2015. 암호화폐 가이드라인 제정
- 2018.10 암호화폐 관련 권고사항 (Recommendation) 변경
- 2019.6 가이드라인 최종안 확정

FATF 'GUIDANCE FOR A RISK-BASED APPROACH TO VIRTUAL ASSETS AND VIRTUAL ASSET SERVICE PROVIDERS'

Section VI VASP 및 가상자산 관련 활동 수행기관에 대한 FATF 국제표준 적용 방안

KYC/RA	▪ 모든 고객 대상 CDD 수행 (거래 수행 전 완료) ▪ CDD 대상거래(최초 거래 시, USD/EUR 1,000 초과 임시거래 시) ▪ 수집대상 정보 : 고객실명 및 추가식별정보(주소, 생년월일, 국가식별번호 등) ▪ 위험기반의 거래모니터링을 통해 의심거래 적발 및 EDD 수행 ▪ CDD정보 기반 고객 프로파일 및 고객 위험 프로파일을 작성하고, 주기적인 업데이트 이행
WLF	▪ PEPs 여부 판단 후 조치 이행
Travel Rule	▪ VA transfer 상 송신/수신자 정보의 수집/보관/제출, 활동 동결, 거래 금지 조치
통제체계	▪ FATF 권고안 도입을 위한 감독당국의 Leadership 필요
TMS/STR	▪ 의심스러운 거래의 보고 ▪ 의심거래 추출 및 FIU에 해당 정보를 보고(혹은 정보접속권한 부여)

"암호화폐 거래소에 대해 **기존 금융권에 준하는** 자금세탁방지 의무 부여"

coindesk

삼정 KPMG

『참고』 FATF 지침서 주요내용 (1/3)

FATF 지침서 섹션 Ⅳ는 가상자산 서비스 제공자(VASP) 및 가상자산(VA) 관련 활동 수행기관이 본 지침 적용 시 고려해야 하는 사항 및 적용방안에 대해 기술되어 있습니다.

섹션 Ⅳ : VASP 및 가상자산 관련 활동을 수행하는 기관에 대한 FATF 국제표준 적용 방안

문단번호	내용 요약
170	FATF 권고안은 VA 관련 서비스를 제공하는 VASP 및 기타 의무기관 모두에게 적용됨
171	ML/TF 위험 완화를 위한 위험식별/평가/효과적 조치를 취해야 함(FATF 권고사항 9~21에 해당되는 내용에 대한 예방 조치 필요)
172	본 지침은 VASP 및 기타 의무기관에 대한 추가적 상세 지침제공을 위한 것임(본 지침에 기술되어 있지 않은 FATF 권고사항이 VASP 및 기타 의무기관에 적용되지 않는다는 의미가 아님)
173	FATF 권고사항 10에 따라 모든 고객대상 CDD를 수행해야 함
174	임계 값 USD/EUR 1,000 이상의 임시거래에 대해서는 CDD를 수행해야 함
175	카지노/귀금속 딜러의 경우 USD/EUR 3,000 이상의 임시거래 혹은 USD/EUR 15,000 이상의 전신송금 임시거래의 경우 CDD를 수행하지만, DNFBP가 VA및 VASP관련 활동(거래)를 수행하는 경우 표준과 동일하게 USD/EUR 1,000 이상 임시거래에 대한 CDD를 수행해야 함
176	최초거래 시, ML/TF 위험 의심 시, 식별된 정보에 대한 정확성 혹은 적절성 의심 시 CDD를 수행해야 함
177	CDD 수행 시 국내법에 따라 고객 실명을 확인해야 하고 필요 시, 추가정보를 수집
178	CDD는 거래수행 전 완료되어야 함

FATF 권고사항 9~21

9. 금융회사의 비밀유지 법률
10. 고객확인 제도
11. 기록보관
12. 고위공직자
13. 환거래은행
14. 자금 또는 가치의 이전 서비스
15. 새로운 기술
16. 전신송금
17. 제3자 의존
18. 내부통제와 해외지점 및 자회사
19. 고위험 국가
20. 의심거래 보고
21. 정보누설과 비밀유지

『참고』 FATF 지침서 주요내용 (2/3)

FATF 지침서 섹션 Ⅳ는 가상자산 서비스 제공자(VASP) 및 가상자산(VA) 관련 활동 수행기관이 본 지침 적용 시 고려해야 하는 사항 및 적용방안에 대해 기술되어 있습니다. (계속)

섹션 Ⅳ : VASP 및 가상자산 관련 활동을 수행하는 기관에 대한 FATF 국제표준 적용 방안

문단번호	내용 요약
179	VASP 및 기타 의무기관은 CDD정보 기반 고객 프로파일 및 고객 위험 프로파일을 작성하고, 주기적인 업데이트가 필요함
180	VASP 및 기타 의무기관은 ML/TF 위험 의심 고객에 대한 블랙리스트(blacklisted wallet addresses)를 관리해야 함
181	CDD는 각국의 규제요구사항에 따라 범위를 축소/확대 등 조정할 수 있음
182	**위험기반의 거래모니터링을 통해 의심거래 적발 및 EDD 수행 가능**
183	거래모니터링은 지속적으로 수행되어야 하며, ML/TF 위험 등을 적발 할 수 있는지 지속적인 확인이 필요함
184	제도적 위험 평가 및 개별 고객 위험 프로파일에 따라 모니터링의 정도를 조정해야 하며, AML/CFT 위험과 모니터링의 연계성에 대해 정기적으로 검토해야 함
185	위험기반접근법(RBA)에 따른 모니터링 시 임계치에 대한 정기적 적합성 검토가 필요하며, 고객 집단에 대한 위험 평가 시 사용되는 기준 및 변수 관련 내용을 문서화하고 해당 문서, 모니터링 결과 및 제기된 문의사항에 대해 관련 당국에 전달해야 함
186	고객의 국내외 **주요 정치적 인물여부를 판단**해야 함
187	**전신송금 관련 의심거래**에 대해 **식별, 보고 및 동결조치**를 수행해야 함

정치적 인물

정치적 인물(PEPs: Politically Exposed Person)

→ 행정, 사법, 국방기관의 고위 관리자, 고위 정치인, 국영기업의 고위 관리자 등이 해당 됨

→ 금융기관은 고객이 국내외 정치적 인물인지 여부를 확인하고 강화된 고객확인(EDD)를 실행해야 함

『참고』 FATF 지침서 주요내용 (3/3)

FATF 지침서 섹션 Ⅳ는 가상자산 서비스 제공자(VASP) 및 가상자산(VA) 관련 활동 수행기관이 본 지침 적용 시 고려해야 하는 사항 및 적용방안에 대해 기술되어 있습니다. (계속)

섹션 Ⅳ : VASP 및 가상자산 관련 활동을 수행하는 기관에 대한 FATF 국제표준 적용 방안

문단번호	내용요약
188	FATF 권고사항 16 준수를 위한 시스템을 규정하지 않았지만, **AML/CFT 의무를 준수할 수 있어야 함**
189	VASP 및 기타 의무기관은 사용 가능한 기술을 통해 FATF 권고사항 16 요건 적용을 고려해야 함
190	VASP 및 기타 의무기관은 **거래 및 고객관련 정보를 보호**하고 안전한 방법으로 관련 당국의 요청 시 정보를 제출해야 함
191	AML/CFT에 대한 효율적인 위험기반접근을 위해서는 **경영진의 참여 및 전사적 위험기반접근의 수행**이 필요함
192	VASP 및 기타 의무기관은 위험 완화를 위한 적절한 AML/CFT 프로그램 및 시스템을 유지/관리해야 함
193	VASP 및 기타 의무기관은 비정상적이거나 의심되는 거래 또는 기금의 이동에 대하여 추가적인 분석을 수행할 수 있어야 함
194	VASP 및 기타 의무기관은 의심되는 VA 또는 VASP가 포함된 거래에 대하여 **신속하게 FIU에 적절한 보고를 취해야 함**
195	가상자산의 전신 송금자 및 수신자 측 모두를 통제하는 VASP의 경우, **의심거래에 대하여 FIU에 보고를 수행하고 송금자 및 수신자측의 정보를 FIU에 제공하여야 함**(해당 정보가 미흡할 경우 이는 의심거래 평가 요소로 고려됨)

권고사항 16 : 전신송금

- 국가는 금융기관이 "발신자에 대해 요구되는 정확한 정보" 및 "수신자에 대해 요구되는 정보"를 전신송금이나 관련 메시지에 포함시키도록 해야 한다. 또한 지급사슬(payment chain) 전반에 걸친 전신송금과 관련 메시지에 해당 정보가 남도록 해야 한다.
- 국가는 금융기관이 "발신자에 대해 요구되는 정보" 그리고/또는 "수신자 정보"의 결손(lack)을 감지할 수 있도록 전신송금을 모니터링하며, 적절한 조치를 취할 수 있도록 해야 한다.
- 국가는 금융기관이 전신송금 과정 상, 테러 및 테러자금의 예방과 근절과 관련되어 UN안보리 결의에 명시된 의무(1999년에 나온 "결의안1267" 및 후속 결의안, 2001년에 나온 "결의안1373" 등)에 따라 지정된 인물/단체를 인지할 경우 즉시 action을 멈추고 거래를 금지하도록 해야 한다.

2. 자금세탁방지체계 도입 필요성

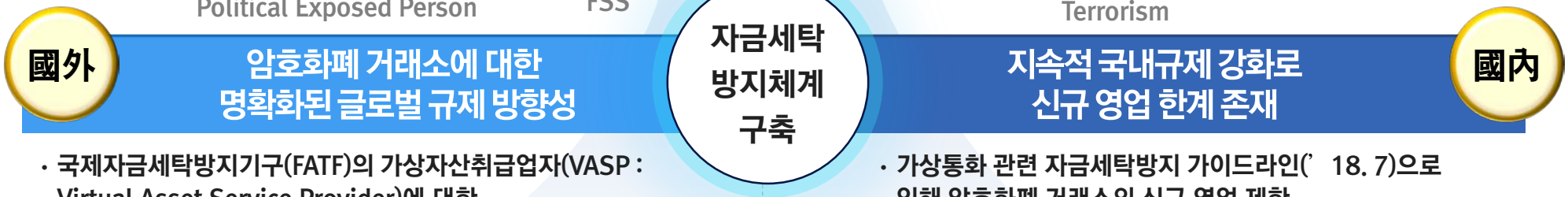
따라서, 자금세탁방지체계의 도입은 제도권 암호화폐 전문 기관으로 위상을 정립하고 규제위험을 최소화하기 위한 필수사항이 되었습니다.

"암호화폐 전문 거래기관으로의 위상정립 및 규제위험 최소화"

01 고객편의를 감안한 위험기반 고객확인제도 도입 ⊕

02 이상거래 모니터링 및 보고체계 구축 ⊕

03 자금세탁방지를 위한 내부통제체계 구축



- 국제자금세탁방지기구(FATF)의 가상자산취급업자(VASP : Virtual Asset Service Provider)에 대한 자금세탁방지의무 명확화('19. 6)
- 글로벌 규제 준수를 통한 제도권 기관으로 도약 가능성 확인

- 가상통화 관련 자금세탁방지 가이드라인('18. 7)으로 인해 암호화폐 거래소의 신규 영업 제한
- 암호화폐 시세 회복에 따른 신규 영업 필요성 증대

coindesk

삼정 KPMG

3. 자금세탁방지체계 구축을 위한 업무범위

암호화폐 거래소에 요구되는 다양한 규제사항을 감안하여, 5개 부문 15개 영역으로 자금세탁방지체계를 구축할 필요가 있습니다.

암호화폐 거래소 관련 규제 요건

- FATF 가상화폐 관련 가이드라인
- 특정금융정보법 및 하위규정
- 위험기반접근법 처리기준 및 내부통제 점검표
- 공중협박자금방지법 및 하위규정
- 특금법 시행령 개정(안)(김병욱 의원)
- 기존 가상통화 관련 자금세탁방지 가이드라인

"6개의 핵심 규제요구 사항을 중심으로 구성"

자금세탁방지체계 구축을 위한 업무범위

SECTION 1 고객확인의무(KYC)
- 신원확인/검증
- 실소유자확인
- 요주의인물대사
- Travel Rule

SECTION 2 위험관리(RISK ASSESSMENT)
- 고객위험평가
- 거래위험평가
- 고위험고객관리

SECTION 3 거래모니터링(TMS/STR)
- Rule 모델
- Alerting & Investigation
- Alert 관리

SECTION 4 AML 전사 및 내부통제
- 전사통제
- 내부통제

SECTION 5 시스템 요건 정의
- 계정계 시스템
- 비대면 채널
- AML시스템

coindesk

삼정 KPMG

coindesk

Contents

자금세탁과 관련된 여러 가지 생각들

자금세탁방지 업무는 다양성에 기초한 보다 적극적 Mind가 가장 중요함. 자금세탁방지 업무는 Compliance 업무 중에서도 가장 주관적 규제 특성을 가지고 있음

규제 시스템?	Negative System (포괄주의)	제한 및 금지규정 나열 / 나머지는 원칙적으로 허용
	Positive System (열거주의)	원칙적으로 모든 것 금지 / 예외적 허용되는 것 나열
사고의 방식?	동양적 사고방식	왜 금융기관이 AML업무를 하나? → 명확한 가이드 요구
	서양식 사고방식	누가해야 할지 명확하지 않은가? → 스스로 증명하는 문화
자금세탁방지를 위해 제일 중요한 것은?	동양적 사고방식	IT 시스템 → 금융기관은 수사기관이 아님
	서양식 사고방식	교육 → 가장 접점에 있는 직원이 가장 잘 알아야 함

자금세탁 이해관계자	자금세탁을 하려는 자	범죄수익 보유자	조직폭력배 등
		탈세를 하려는 자	기업(인) / 고액자산가
		불법자금 보유자	정치인 / 유력인사 등
	자금세탁을 도와주는 자	매개자	브로커 / 금융기관종사자
	규제하려는 자	규제기구(국가)	국제기구 / 미국
	규제를 피하려는 자	피해자	각 국가 / 금융기관(종사자) 등

coindesk

삼정 KPMG

1. 고객확인제도 (Know Your Customer) 란? (1/2)

KYC는 **고객의 정보를 획득하고 신원을 확인/검증하는 제도**로서 고객의 자금세탁관련 혐의성을 판단하기 위한 기초정보를 수집하는 제도입니다.

KYC 수행절차

저위험

고객확인의무

CDD Customer Due Diligence

기본적인 신원확인 정보를 확인하고 검증하는 간소화된 고객확인의무 적용

강화된 고객확인의무

EDD Enhanced Due Diligence

거래목적 및 용도 파악을 위한 추가 정보를 요청하고 검증하는 강화된 고객확인의무 적용

고위험

KYC 수행목적

고객의 **자금세탁 위험에 기반**을 둔 **차별화된 고객확인정보**의 획득

KYC 효과

자금세탁 불법 행위의 사전적 차단

고위험 고객의 거래목적 및 용도를 파악함으로 잠재적 자금세탁 시도를 사전적으로 차단

의심스러운 거래 보고 효율성 제고

고위험 고객에게 추가로 질의한 정보를 추후 의심스러운 거래 보고 여부 판단 시에 이용

자금세탁 위험의 효과적 관리

고객 정보, 거래 정보를 이용하여 고객의 자금세탁 위험을 평가 후 차별화된 고객 정보를 획득

금융기관의 건전성 제고

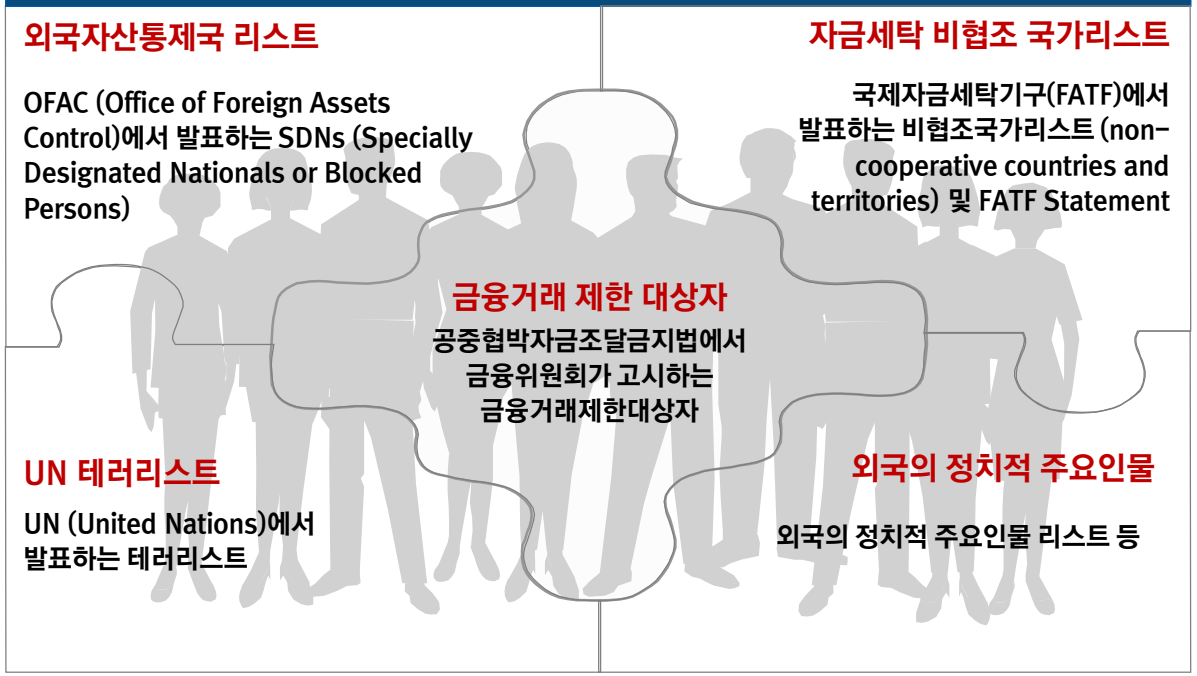
자금세탁 위험, 평판, 운영, 법률 위험을 효과적으로 관리하여 금융기관의 건전성 제고

1. 고객확인제도 (Know Your Customer) 란? (1/2)

통상적으로는 KYC에는 CFT(Counter Financing of terrorism:공중협박자금관리)를 위한 요주의인물대사가 포함됩니다.

요주의인물대사는 테러자금 연루 예방을 위해 금융위원회가 고시한 금융거래제한 대상자 및 국외에서 발표된 테러리스트 명단 등과 고객을 대사하는 것을 의미

주요 요주의인물의 구성



외국자산통제국 리스트

OFAC (Office of Foreign Assets Control)에서 발표하는 SDNs (Specially Designated Nationals or Blocked Persons)

자금세탁 비협조 국가리스트

국제자금세탁기구(FATF)에서 발표하는 비협조국가리스트 (non-cooperative countries and territories) 및 FATF Statement

금융거래 제한 대상자

공중협박자금조달금지법에서 금융위원회가 고시하는 금융거래제한대상자

UN 테러리스트

UN (United Nations)에서 발표하는 테러리스트

외국의 정치적 주요인물

외국의 정치적 주요인물 리스트 등

수행 내용

- 금융거래완료 前 요주의 인물 확인을 수행
- 계좌 신규, 일회성 금융거래 등을 대상으로 수행
- Watchlist Filtering 대상자
  - ➢대리인 거래시 대리인/본인 모두 Watchlist Filtering 수행
  - ➢해외 전신송금의 경우 수취인(송금인) 양자에 대한 Watchlist Filtering 도 수행

"금융거래관계 및 용역 / 물품 계약관계" 를 제한

coindesk

삼정 KPMG

2. VASP에의 KYC 도입의 의미

암호화폐 거래소의 KYC 도입은 단순한 규제의 추가가 아닌, 고객 접촉 및 대고객 업무절차의 변경을 의미합니다.

KYC를 도입한다는 것은?

도입 이후, 암호화폐 거래에 앞서 수집할 개인정보는?	
고객확인 정보	**검증관련 정보**
성명	신분증정보
실지명의(주민번호)	고객계좌정보
주소	IP정보
연락처	
직업	
실소유자 정보	
공개키 정보	

: 기존 수집 정보

거래에 앞서 다양한 고객정보 수집절차 필요

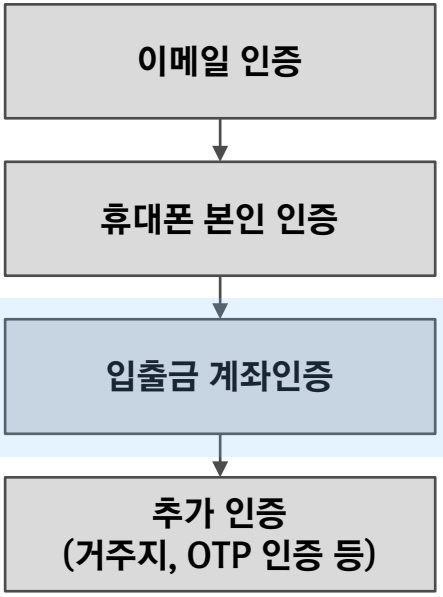
고객정보 입력에 따른 유저 편의성 저하

모바일 중심 금융기관의 핵심가치인 편의성과 상충

올바른 KYC 도입방향은?

기존 인증절차와 고객확인절차와의 통합 검토 필요

[암호화폐 거래소 본인인증절차]



기존 실명확인 계좌인증을 비대면 실명확인 절차와 통합운영

주) 본인인증절차는 거래소별로 상이할 수 있음

3. KYC 도입 시 핵심 고려사항

암호화폐 거래소의 효율적 KYC도입을 위해 비대면 실명확인절차를 준용한 KYC 절차, 기존 고객 대상 KYC 수행 거래 정의 등이 필요합니다.

KYC 도입을 위한 핵심 고려사항

1 금융실명법 미적용 기관

- 금융기관과 같은 실명확인절차가 명확하지 않은 암호화폐 거래소에 대한 KYC 도입
- 현재 금융실명법 미적용 금융거래에 대해서도 신분증을 통한 실지명의 정보 수집 중(신용카드, 보험, 대출 등)

2 암호화폐 거래소 채널 특수성 – 비대면

- 비대면 채널 위주의 암호화폐 거래소 특수성 고려 필요
- 현행 비대면실명확인 절차를 준용하되, 신속한 거래를 원하는 고객의 편의성을 고려해야 함

3 기존 고객의 KYC 수행 이슈 존재

- 신규 고객 뿐만 아니라, 기존고객(법령 개정 전 기존 거래 이력이 존재하는 고객)에 대한 KYC 고려 필요

KYC 효율적 도입방안

Solution 1 비대면 실명확인절차를 준용한 KYC 절차 설계

- 모바일/Web 등 비대면 채널로 유입되는 고객에 대해서는 EDD 수행을 원칙으로 비대면 실명확인 절차에 준하는 KYC 절차를 진행 (現 금융기관 비대면 채널 및 인터넷 전문은행 등 운영현황 고려)
- 대면 채널 존재 시 대면 중심 KYC 절차를 Two-Track으로 운영

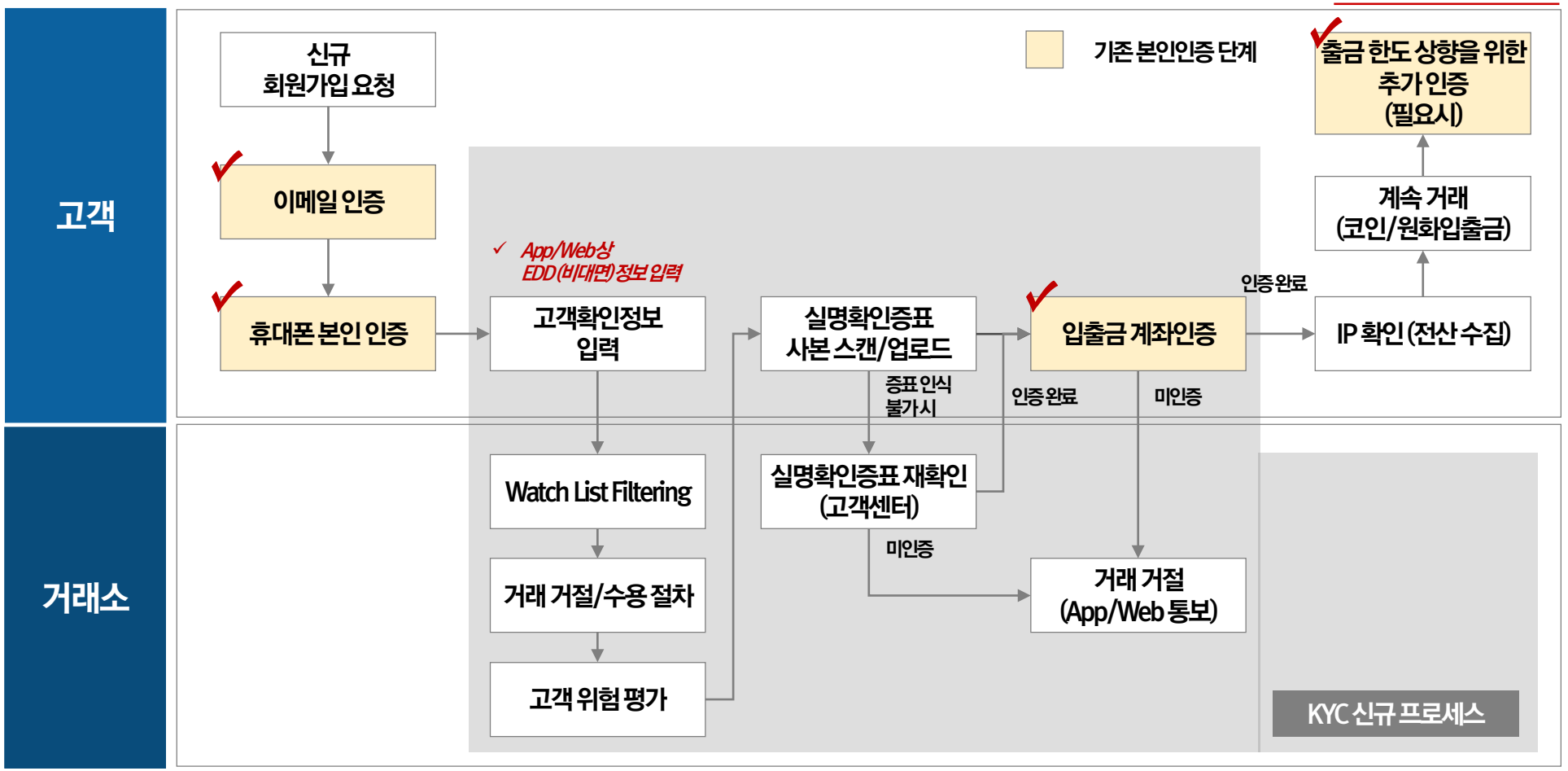
Solution 2 규제를 고려한 KYC 대상 및 거래 정의

- 신규 고객 및 기존 고객 대상 KYC 대상 고위험 거래 정의 필요
- 매체 변경 시 혹은 거액 코인/원화 출금 거래 시 등

3. KYC 도입 시 핵심 고려사항 – KYC 수행절차

비대면 채널로 유입되는 신규 고객에 대해서는 EDD 수행을 원칙으로 비대면 실명확인 절차에 준하는 KYC 절차를 진행합니다.

Illustrative Only



『참고』 비대면 실명확인절차 적용 방안

비대면 실명확인을 위하여 금융위원회에서 제시한 상세 실명확인 절차 중, 기존계좌를 활용한 방법을 포함하여 실명확인증표 사본 제출 또는 영상 통화 등의 방식을 활용하여 실명확인절차를 정의할 수 있습니다.

** 출처 : 금융위원회*

	실명확인 방법	필수 여부	설명	장점	단점
1	실명확인증표사본 제출	필수 2개 선택	실명확인증표 사진 및 스캔 후 신분증진위확인 서비스 이용하여 확인	▪ 실명증표 기반 PC, 스마트폰 활용 편리한 비대면 인증 가능	▪ 진위확인이 어려울 수 있음 ▪ 업무 처리에 따른 고객 불편 高
2	영상 통화		고객과 영상통화를 실시하여 사진과 대조	▪ 육안 대조를 통한 신뢰성 높음 ▪ 영상통화 수령을 통한 고객 편의도 제고 가능	▪ 고객센터 상주직원 관리 필요 및 업무시간 외 확인이 어려움 ▪ 고객 영상장비 미보유시 확인 어려움
3	현금카드 전달 때 확인		현금카드, 보안카드, OTP 등 접근매체 전달 시 실명확인 수행	▪ 전달업체 직원을 통한 대면 확인 가능	▪ 실물 전달을 위한 인력 필요 및 상당 시간이 소요
4	기존계좌 활용		기존 금융계좌를 이용, 소액을 이체하도록 하여 실명확인 수행	▪ 활용 범위가 넓고 간단함	▪ 명의도용 가능 및 복수 계좌 개설 가능
5	기타 이에 준하는 방법		지문인식, 정맥 등 바이오 인증과 같은 필수 인증 기술에 준하는 인증 기술 적용	▪ 바이오 인증 신기술 적용 가능	▪ 안전성 검증 어려움
6	다수의 개인정보 검증	권고	고객이 제공하는 개인정보와 신용정보사 등이 보유한 정보를 대조	▪ 고객 입장에서 사용 간편 및 금융회사 적용이 쉬움	▪ 개인정보 관리 어려움 및 사고 유출 시 리스크 존재
7	타 기관 확인 결과 활용		공인인증서, 아이핀 등 타 인증기관에서 신분 확인 후 발급된 결과 활용	▪ 기 사용 기술 활용을 통한 편의성 및 범용성이 높음	▪ 분실 시 유출 가능성 및 사고 발생시 책임 소재 분쟁 이슈

3. KYC 도입 시 핵심 고려사항 – KYC 대상 및 거래 정의

암호화폐 거래의 특성을 고려하여 고객확인의무 대상 거래를 암호화폐 거래를 위한 회원가입, 원화/코인 출금거래, 매체 및 고객정보 변경 거래로 정의할 수 있습니다.

규제 요구사항

1 FATF Guidance

- 가상자산의 경우 아래의 경우 KYC를 수행해야 함
  1. 비즈니스 관계 수립
  2. 특정 금액 이상의 비정기적 거래(USD/EUR 1,000) 수행 시
  3. 고객 정보의 정확성 또는 적절성에 의문이 생긴 경우

2 특금법 시행령 / AML 업무규정

- 고객확인의무 적용 범위
  1. 계좌의 신규 개설 2. 일회성 금융거래
- 기존 고객의 고객확인 시기
  1. 자금세탁행위등의우려가 높은 거래가 발생하는 경우
  2. 고객확인자료 기준이 실질적으로 변한 경우
  3. 계좌운영방식에 중요한 변화가 있는 경우
  4. 고객에 대한 정보가 충분히 확보되지 않았음을 알게 된 경우

고객확인의무 대상 거래 정의 예시

구분 / 거래유형	KYC 수행대상	일회성 금융거래	주요 정보 변경
회원가입	O	대상 외 (일회성 금융거래의 정의 상 KYC 이력이 없는 기존 고객은 존재하나 일시적 거래는 없음)	–
원화입금	–		–
코인입금	–		–
에어드랍	–		–
매매	–		–
원화출금	△(금액기준)		–
코인출금	△(금액기준)		–
매체 및 고객정보 변경	–		O

고객불만 가능성 및 규제 요구사항 검토 후 확정 필요

3. KYC 도입 시 핵심 고려사항 – 신원확인항목 정의

규제 요건에 따라 고객 유형별 신원확인 대상 항목을 정의하고 신원확인 절차를 수립해야 합니다.

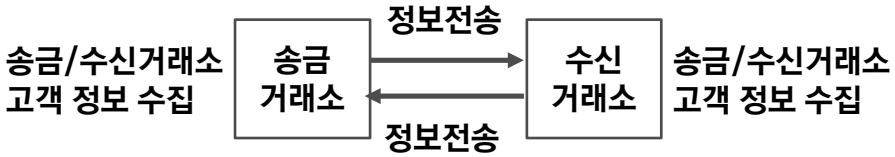
	CDD /EDD	신원확인 대상	신원검증 대상	관련 법령			AS IS	TO BE
				특금법	FATF 지침	자율규제안	수집 단계	수행 방안
성명(한글명)	CDD	O	O	O	해당 국가 법령에 따름	O	휴대폰 인증시	현행 유지
성명(영문명)		O	O	O		O	–	KYC 이행시 수집
실명번호		O	O	O		O (관련법령에 따름)	–	실명확인증표 촬영 시
주소		O	O	O		O	한도 상향시	KYC 이행시 수집
연락처		O	O	O		O	휴대폰 인증시	현행 유지
생년월일(외국인)		O	–	O		–	휴대폰 인증시	현행 유지
성별(외국인)		O	–	O		–	휴대폰 인증시	현행 유지
국적		O	–	O		–	–	KYC 이행시 수집
실소유자		O	–	O		–	–	KYC 이행시 수집
직업 및 업종		O	–	O		–	한도 상향시	KYC 이행시 수집
거래목적	EDD	O	–	O		–	한도 상향시	KYC 이행시 수집
거래자금원천		O	–	O		–	한도 상향시	KYC 이행시 수집
IP Address		O	–	–	O	–	로그인/아웃, 원화 입출금시 IP 수집	KYC 이행시 수집 (전산 자동 추출)

4. VA Transfer에 대한 주의의무 – 개요

기존 금융기관의 전신송금 주의의무가 VA transfer로 확대됨에 따라, 거래소 간 코인 이동 시 고객정보를 수집/보관/제출할 수 있는 방안을 확보해야 합니다.

VA Transfer 관련 요구사항(Recommendation 16)

1 VA transfer 시 고객정보*를 수집하고 전송



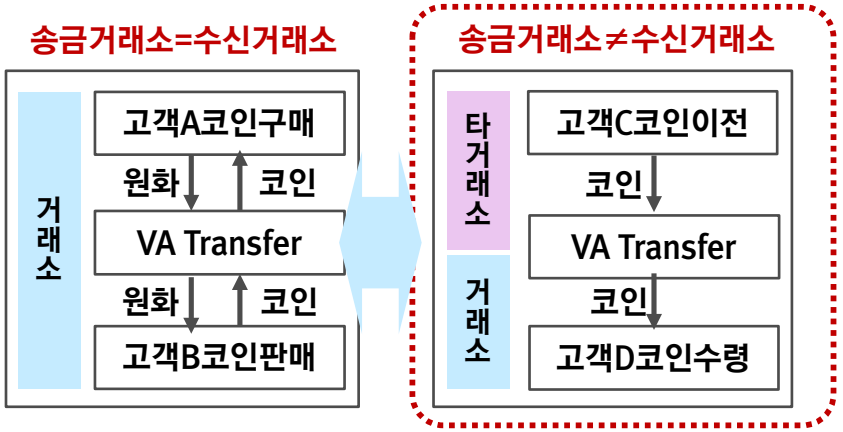
*고객정보
- 송금거래소 고객명
- 송금거래소 고객 VA지갑 주소
- 송금거래소 고객 생년월일 또는 주소 또는 국가식별번호 또는 고객식별번호
- 수신거래소 고객명
- 수신거래소 고객 VA지갑 주소

2 수집정보 기반으로 거래 모니터링 → 거래 금지 지정인물일 경우 거래 중단

3 규제당국의 요구에 따른 정보 제출

정보 수집 방안 확보 필요성

분산원장 사용에 따른 정보 전달 어려움



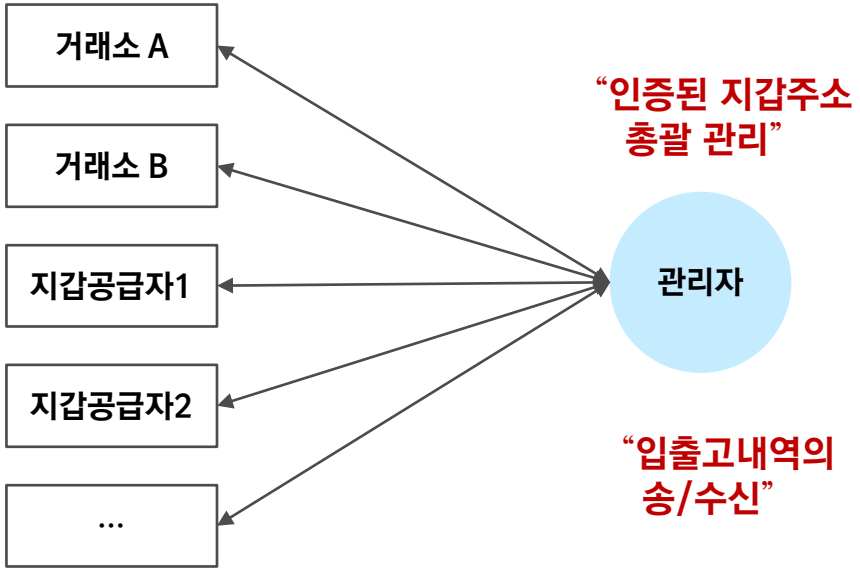
송금 및 수신거래소가 모두 당사에 해당하는 경우, 최초 가입 시 旣수집된 고객 정보 이용 가능

타 거래소에서 입수되는 코인의 경우, 해당 코인 보유 고객정보가 입수 필요하나, "분산원장 사용에 따라 정보 전송이 어려움"

4. VA Transfer에 대한 주의의무 – 적용(안) 예시

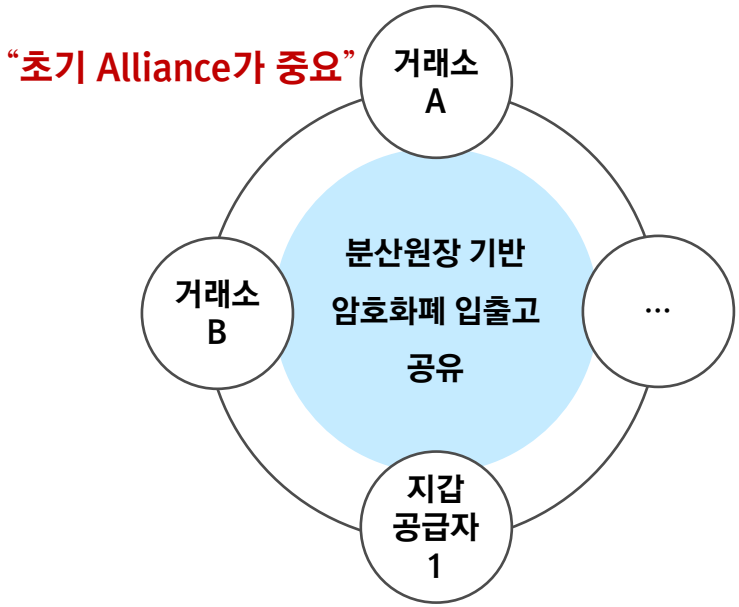
현재, Travel Rule에 대응하기 위한 다양한 방안이 논의되고 있으며, **중앙집중형 네트워크 방식** 혹은 **거래소 간 Alliance**를 통한 이체내역을 공유하는 분산원장 체계 등을 고려할 수 있습니다.

1. 중앙집중형 네트워크 인프라 구성



- 전통적 방식의 높은 거래비용
- 입출고 관리자의 수행주체(협회 or 거래소)에 따른 갈등 존재
- 입출고 관리자에 대한 강한 통제 필요(낮은 확장 가능성)

2. 거래소 간 White/Black List 공유



- 폐쇄형 분산원장을 통한 비교적 낮은 거래 비용
- 입출고 수행주체에 따른 갈등 낮음
- 글로벌 거래소 등과 협업 가능성 높음

coindesk

삼정 KPMG

5. 요주의인물 대사 – 핵심 고려사항

효율적 요주의인물 대사를 위해서는 비대면 전문기관에 적합한 고객수용절차를 수립하고, 적출가능성에 대한 사전점검이 필요합니다.

요주의인물 대사 핵심 고려사항

1 거래 거절/승인에 대한 전결권 정의 필요

- 비대면 전문 기관의 특성 상, Business Line 상 고위경영진(본부장)의 적용 불명확
- 거래중지 절차 설계 시 고객센터 등과 연계한 효율적 프로세스 필요

2 기존 고객에 대한 적출 가능성 점검 필요

- 비거주자/외국법인 등으로 인한 적출 가능성 증대
- 기존 고객의 WLF적출 가능성에 대한 사전 점검 및 규모에 적합한 업무프로세스 설계 필요
- Watch List 획득 및 관리방안 설계 필요
  - OFAC SDN에 지갑주소 포함에 따른 Filtering 기능 검토

WLF 효율적 도입방안

Solution 1 비대면 거래에 특화된 거래수용 절차 도입

- 요주의 인물 매칭 시 "일시 거래중지 → 콜센터에 의한 동일인 판정 및 PEPs 추가 EDD수행 → AML소관부서에 의한 점검" 절차로 설계 (WLF와 연계한 콜배분 기능 필요)
- 고객 수용을 위한 고위경영진에 대한 정의(전결절차) 필요

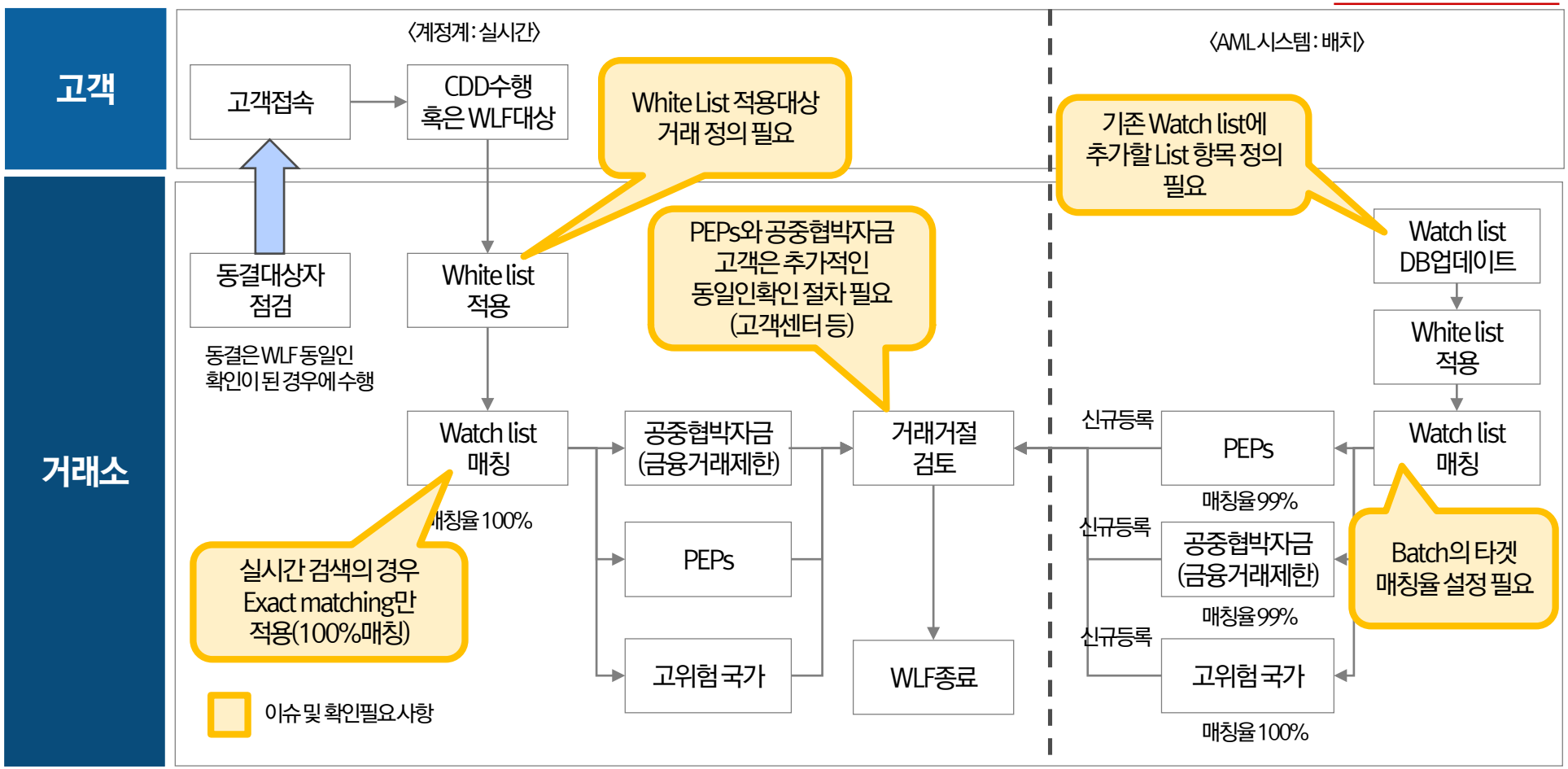
Solution 2 Watch List 적출 가능성에 대한 사전 분석

- 국내 PEPs에 대한 범위 및 적출 가능성에 대한 사전 점검 필요
- 요주의 리스트 획득 및 관리 방안(상용 DB 등)에 따른 적출 가능성 분석 필요

5. 요주의인물 대사 – 수행방식

암호화폐 거래소에 적용 가능한 요주의인물 대사절차의 구체적 예시입니다.

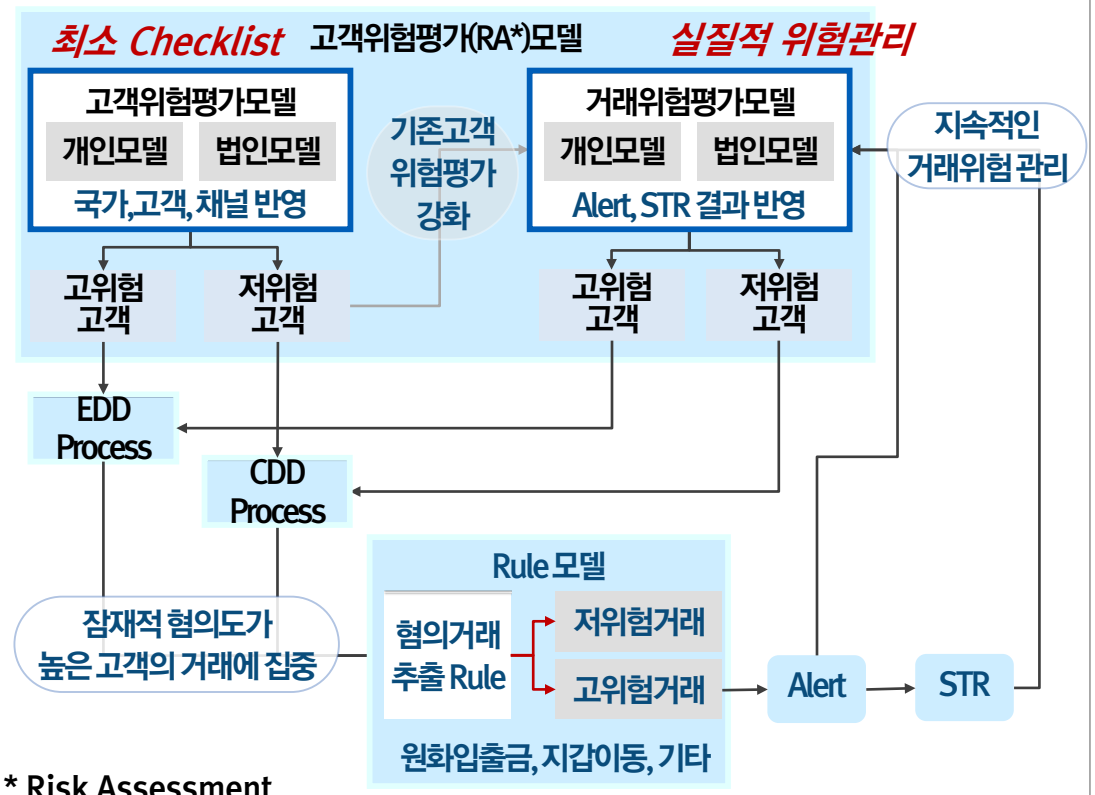
Illustrative Only



6. 고객 위험평가모델 구조

고객 위험평가모델은 Initial Model과 Behavior Model로 구성되며 비대면 채널의 특성을 고려하여 고객 자체의 위험도 보다는 거래에 중점을 둔 위험관리체계를 수립합니다.

위험평가모델 구조



위험평가모델 상세 설명

1 당연 고위험

- 자금세탁업무규정 상 고위험으로 명시된 대상
- 외국의정치적주요인물, 공중협박자금조달고객, FATF 비협조국가 국민 등

2 고객위험 평가 (I 모델)

- 고객의 고유 위험 (고객/국가/보유 상품 등) 평가 수행
- 최초 고객 회원가입 시, KYC 재이행시, 고객의 정보 변경시 위험평가 재수행

3 거래위험 평가 (B 모델)

- 고객이 수행한 거래에 대한 위험평가
- TMS 모델 내 Rule 에 대한 Alert 정보를 기반으로 일별 평가

coindesk

Contents

실질적 경감방안은?

최근의 자금세탁방지 업무는 일반적 자금세탁방지 통제를 넘어 각 금융기관 등에게 영위하는 전체 업무에 대한 특화된 통제를 요구하고 있는 것이 일반적 추세임

- 정책 및 절차
- 역할 및 책임
- 위험 평가
- 직원 교육 및 인식

- 고객확인제도
- 코레스뱅킹 릴레이션십
- 거래 스크리닝
- 거래 모니터링

- 무역금융 프로파일
- 위험신호
- 민군 겸용 물자
- 문서 사기

기술의 뒷받침_혁신(Innovation)

최근 감독기관들은 자금세탁방지 업무수행을 위해 금융기관 등이 혁신적 모니터링을 방안 도입을 장려하고 있으며, 이에 대해 긍정적 평가를 내리고 있음

- 규제 당국은 금융 범죄 준수를 위한 '블랙박스' 솔루션을 채택하기를 꺼리는 반면, 일부(예: MAS / Monetary Authority of Singapore)는 업계와 협력하여 감독이 가능한 기계학습의 새로운 활용(예: 제재 심사 영역)을 모색 중
- 영국에서는 FCA가 핀테크 부문과 협력하고 있으며, 최근 미국 5개 연방 감독기관은 은행(아래에서 정의한 바와 같이)이 AML 준수 의무를 충족하기 위해 **"혁신적인 접근법을 고려하고, 평가하고, 그리고 적절한 경우 책임감 있게 구현할 것"**을 권장하는 내용의 공동 성명을 발표

공동성명에는 다음과 같은 내용이 포함됨 :

- 은행들은(유효한 프로그램을 유지하면서) 규정 준수에 대한 **혁신적 접근법을 추구한다고 해서 비판 대상이 되지 않을 것임**. 그리고,
- 규정 준수 프로그램과 격차가 노출되는 파일럿 프로그램이 반드시 그것으로 인해 감독 조치를 취하는 결과를 가져오지는 않을 것. 예를 들어 은행이 인공지능 기반 거래 모니터링 시스템을 테스트 또는 구현하고 기존 프로세스에서는 식별되지 않았을 의심스러운 활동을 식별하는 경우, 감독기관은 은행의 기존 프로세스가 부족하다고 자동적으로 가정하지는 않을 것

1. 의심거래보고제도 (Suspicious Transaction Report) 란?

STR은 **의심스러운 고객/거래에 대해서 금융정보분석원에 관련 정보를 보고**하는 것을 의미합니다.

의심거래보고제도 (STR : Suspicious Transaction Report)

업무 수행 중 포착한 자금세탁행위가 의심스러운 거래, 정황 등에 대하여
금융정보분석원(KoFIU) 및 수사기관에 그 내용을 보고하는 자금세탁방지의 핵심 제도

- 금융거래 관련 수수한 재산이 불법재산이라고 의심되는 합당한 근거가 있거나, 거래상대방이 자금세탁행위를 하고 있다고 의심되는 합당한 근거가 있는 경우, 개별 금융기관이 금융정보분석원(KoFIU)에 보고하는 제도

2. TMS/STR 도입 시 핵심 고려사항

암호화폐 거래소 채널의 특수성 및 비대면 채널의 특징을 고려하여 의심스러운 거래 적발을 위한 거래 모니터링 모델 및 보고/관리체계를 수립합니다.

TMS/STR 핵심 고려사항

1 거래소 협의거래 유형 불명확

- 일반 금융권의 경우 장기간 축적된 자금세탁 사례를 기반으로 자금세탁 협의거래 유형 존재 → Rule 도출이 상대적으로 용이
- 암호화폐 거래소의 경우 의심스러운 거래보고 Rule에 활용가능한 사례가 부족 → 기존 금융권 Rule Pool을 최대한 활용하는 한편, 암호화폐 거래 고유 특성을 반영한 신규 Rule 도출

2 암호화폐 거래소 채널 특수성 고려

- 비대면 채널 특수성 고려한 TMS/STR 운영 프로세스 설계 필요
  → 영업점 등 타 부점에 Alert 배분 불가
- 암호화폐 거래량 多 → Alert 과다 발생으로 인한 STR 검토 및 보고 업무 부담 증가 우려

TMS/STR 수립방향

Solution 1 암호화폐 거래소 특수성을 반영한 Rule 도출

1) 기존 금융권 Reference Rule Pool 활용
2) 암호화폐 거래소 특성 반영한 Rule 신규 도출

→ 원화 입출금 등 기존 금융권과 유사한 거래의 경우 벤치마크 Rule 활용

→ 암호화폐 자산이동 등 암호화폐 거래소 특수 거래의 경우 업무 프로세스에 적합한 고유 Rule 도출 (KYT Solution 활용 등)

Solution 2 TMS/STR 운영 프로세스 구축 시 편의기능 구현

- 중앙집중형 STR Investigation 및 보고 프로세스 마련

→ AML 주관부서에의 집중도 감안하여 Alert 우선순위 설정

→ Alert 발생 거래에 대한 STR 대상여부 판단을 용이하게 하기 위해 의심여부 판단 기준 정의

『참고』 FATF 규제요건

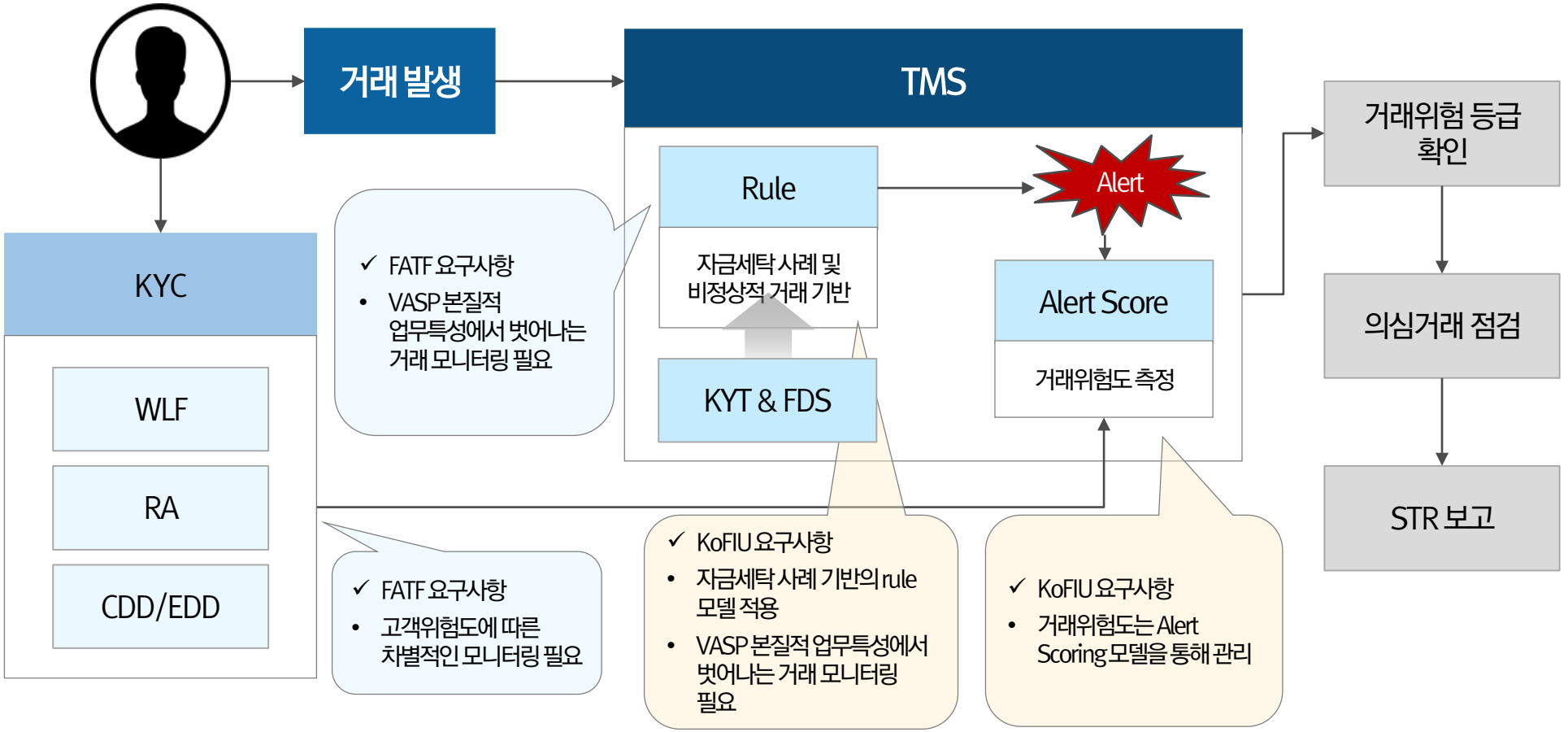
FATF에서는 기존 금융권에 준하는 수준의 TMS체계를 암호화폐거래소에 요구하고 있습니다.

TMS 관련 FATF 요구사항	시사점
124. 자금이 범죄 수익이거나, 테러 자금 조달과 관련이 있다고 의심할 만한 근거가 있거나 의심되는 경우 모든 금융기관은 해당 FIU에 의심내역을 신속하게 보고할 것을 요구 (STR 제출)	➢ 기존 금융기관에 준하는 TMS 설계 필요
182. 거래모니터링: 거래의 성격이 VASP (가상자산 서비스 제공자)의 고객, 본질, 비즈니스 상의 목적과 부합하는지 조사. 고객 프로파일에 대한 변경사항을 파악하고 EDD가 필요한지의 여부를 조사	➢ VASP 본질적 업무특성에서 벗어나는 거래 모니터링 필요
184. 개별 고객 위험 프로필에 따라 모니터링 범위와 정도를 조절해야 함. 고위험 상황에는 강화된 모니터링이 필요하며, 강화된 모니터링은 VASP, 고객 또는 고객의 거래상대방과의 즉각적인 거래까지 확장되어야 함	➢ 고객 위험도에 따른 차별적인 모니터링 필요

FATF의 지침은 암호화폐 거래소에 대해 TMS/STR 의무만을 규정(상세 절차 미정의)
즉, 현시점에서는 현재 금융권과 유사하게 TMS를 설계해야 함

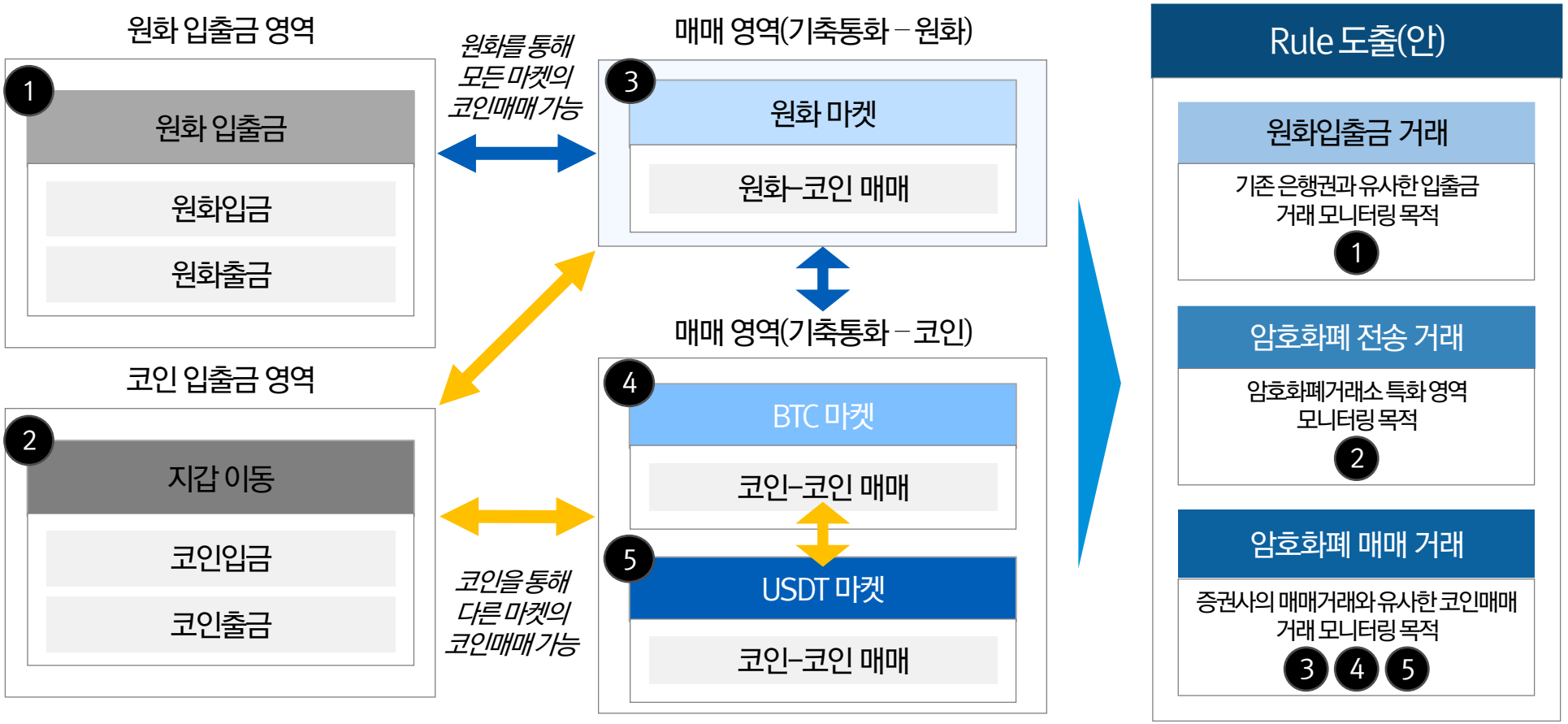
3. VASP를 위한 TMS 구조 예시

TMS는 Rule모델을 기반으로 Alert을 발생 시킨 후 고객/거래위험 평가결과 및 Alert등급을 활용하여 효율적인 거래조사가 가능한 구조로 구성할 수 있으며, 필요 시 KYT Solution 혹은 FDS 결과 등을 활용합니다.



4. 암호화폐 거래 구조에 따른 Rule 도출 방안

암호화폐 거래는 원화 입출금 영역, 코인 입출금 영역, 매매영역으로 구분 할 수 있으며, 각 영역의 특성에 적합한 Rule을 적용 및 도출하여야 합니다.



5. 의심거래 룰(Rule) 도출 예시

암호화폐 거래(입출금 및 매매)에 최적화된 모니터링 체계를 구현하기 위해 벤치마크 및 내부관리 위험요소 등을 활용해 의심거래 룰을 도출합니다.

Illustrative Only

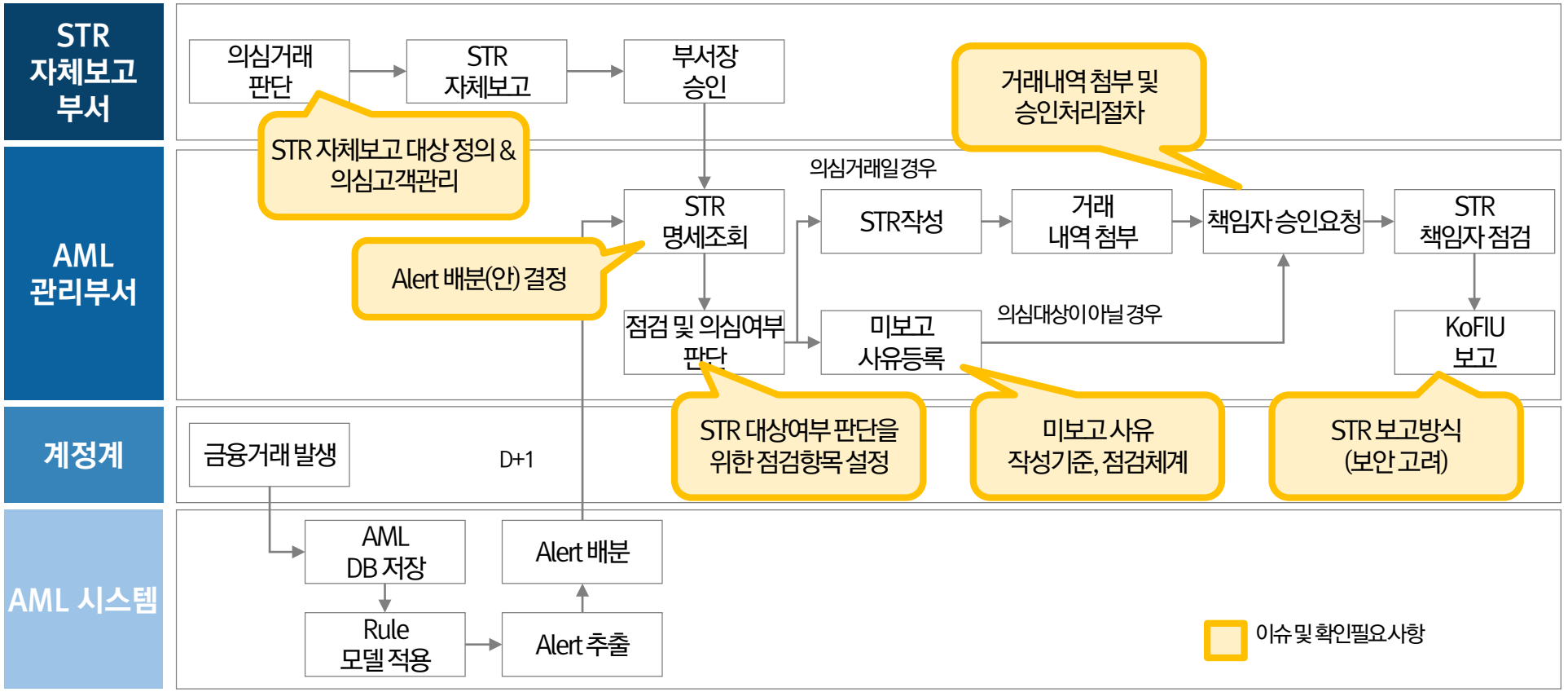
거래 유형	Rule 상세 설명
공통	고령투자자 (만 70세 이상) 중 1. 최근 1개월 간 거래금액(매수/매도 각각)이 500만원 이상이거나, 2. 최근 7일 간 원화/코인 입출금 거래가 30건 이상인 계정
공통	동일한 이메일 주소/휴대폰번호가 3개 이상의 실명번호에 등록되어 있을 때, 해당 이메일 주소/휴대폰번호를 등록한 고객
입출금 거래	최근 1개월 간 매매거래가 없는 계정 중 원화/코인 입출금 거래가 10회 이상 발생한 계정
입출금 거래	최근 7일 간 원화/코인 입금액이 10억 원 이상인 개인 계정
입출금 거래	계정 생성 당일 원화/코인 1억 원 이상 입금한 후 7일 동안 입금액의 90% 이상 출금한 고객
입출금 거래	최근 7일 간 5억 원 이상 코인 이동 거래(입출금)한 고객 중 거래대상 지갑주소가 5개 이상인 고객
입출금 거래	최근 1일 동안 동일 지갑주소에게 건별 1천만원 이상 합계 1억 원 이상 코인을 송금한 고객
입출금 거래	KYT Score에서 Red로 적출되는 입출금거래
입출금 거래	최근 7일 간 법인계좌에서 합산 10억 원 이상 개인계좌로 코인 송금한 거래
매매 거래	투자유의종목 지정 후 최근 1일 해당 코인을 매수거래한 계정
매매 거래	최근 3일 간 매매거래금액 합계가 2억 원 이상인 계정 중에서, (최근 1개월 시점 기준) 직전 2개월 간 거래가 없는 계정
매매 거래	최근 1개월 간 수익액이 10억 원 이상이고 수익액의 90% 이상이 출금된 고객
. . .	. . .

6. STR 보고 프로세스

비대면 기관 특수성을 고려하여 의심거래 보고 운영 및 관리 프로세스를 수립하고, 예상되는 이슈 사항에 대한 대응 방안 마련이 필요합니다.

Illustrative Only

TMS/STR 운영 프로세스 및 주요 이슈사항 (예시)



coindesk

Contents

1. 거래소 업계 공통 이슈 사항

향후, 암호화폐 거래소의 성공적인 AML도입을 위해서는 거래소의 특수성을 반영한 규제 방향성 정의 및 상세 적용을 위한 논의가 필요합니다.

주요 논의 필요사항	상세 내용
실명확인 입출금 계좌 신고수리 요건	✓ 거래소 신고 수리 요건에 실명확인 가상계좌 발급 의무 포함(발급조건은 시행령에 명시) ✓ 일정 조건 충족 시 은행이 무조건 가상실명계좌를 발급하는 방향으로 논의 진행 중
비거주자 기존 고객	✓ 기존 휴대폰 인증을 통해 유입되었던 비거주자 고객의 신원 검증 방안 논의 필요 ✓ 비대면 실명확인 시 여권은 실명확인증표로 인정되나, 실시간 검증은 불가
실명확인증표 수집	✓ 금융기관과 같은 실명확인절차가 명확하지 않은 암호화폐 거래소에 대한 KYC 도입 시 실명확인증표 수집 이슈 존재 (단, 현재 금융실명법 미적용 금융거래에 대해서도 신분증을 통한 실지명의 정보 수집 중 (e.g 신용카드, 보험, 대출 등))
실시간 신원검증	✓ 기존 금융기관의 경우, 금융결제원을 통한 신분증 진위여부 실시간 검증 가능 ✓ 거래소의 경우 금융결제원 망 이용 불가 시 신원검증정보 지연가능성 존재

삼정 KPMG

Contacts

The contacts at KPMG in connection with this report are:

Risk Consulting Services
Governance, Risk & Compliance Team

문철호 상무이사
02-2112- 0869
010-3378-7086
cmoon@kr.kpmg.com

삼정 KPMG

감사합니다.

kpmg.com/kr

kpmg.com/socialmedia

kpmg.com/app