14 сентября 2021

SWIFT CSP
так ли все сложно?

АНДРЕЙ СТЕПАНОВ
Начальник Управления информационной безопасности
Банк СОЮЗ (АО)
Andrey.Stepanov@banksoyuz.ru

БАНК СОЮЗ

Society for Worldwide Interbank Financial Telecommunications (SWIFT)

SWIFT — международная межбанковская система передачи информации и совершения платежей.

Альянс основан в 1973 году; соучредителями выступили 248 банков из 19 стран. Штаб-квартира SWIFT находится в Бельгии, недалеко от Брюсселя. SWIFT является кооперативным обществом, созданным по бельгийскому законодательству, принадлежит его членам. По состоянию на 2021 год, членами SWIFT являются более 11 тыс. финансовых организаций в более чем 200 странах мира, в том числе около 1000 корпораций. Средний оборот более 30 млн сообщений в день.

Адресация абонентов в системе основана на так называемом BIC (англ. Business Identifier Code, ранее известном как Bank Identifier Code), присваиваемом в соответствии с международным стандартом ISO 9362. Также иногда именуется SWIFT-BIC, SWIFT ID или SWIFT code. На практике для совершения платежа в Европе достаточно знать наименование и IBAN-код банковского счета получателя (уже содержащий интерпретированный BIC в своём составе).

Инциденты в SWIFT

Хищение из банка Бангладеш

2016г. Хакеры смогли взломать систему финансовых транзакций SWIFT, которая используется в качестве стандарта для межбанковского взаимодействия.
Хакеры пытались вывести из банка южно-азиатской страны $951 млн. Большая часть транзакций была заблокирована, однако $81 млн все уже удалось вывести на счета игорных заведений на Филиппинах, после чего следы этих денег были потеряны.
Источник
https://www.cnews.ru/news/top/2016-04-25_hakery_vzlomali_swift

Хищение из российского банка

15 декабря 2017 года была зафиксирована успешная кибератака на один из российских банков с выводом денег за рубеж через международную систему передачи финансовой информации SWIFT. В обзоре FinCERT говорится: «В Банк России направлена информация об одной успешной атаке на рабочее место оператора системы SWIFT. Объем несанкционированных операций в результате данной атаки составил 339,5 миллиона рублей»
Источники
https://habr.com/ru/post/345058/
https://www.kommersant.ru/doc/3501353

SWIFT Customer Security Programme (CSP)

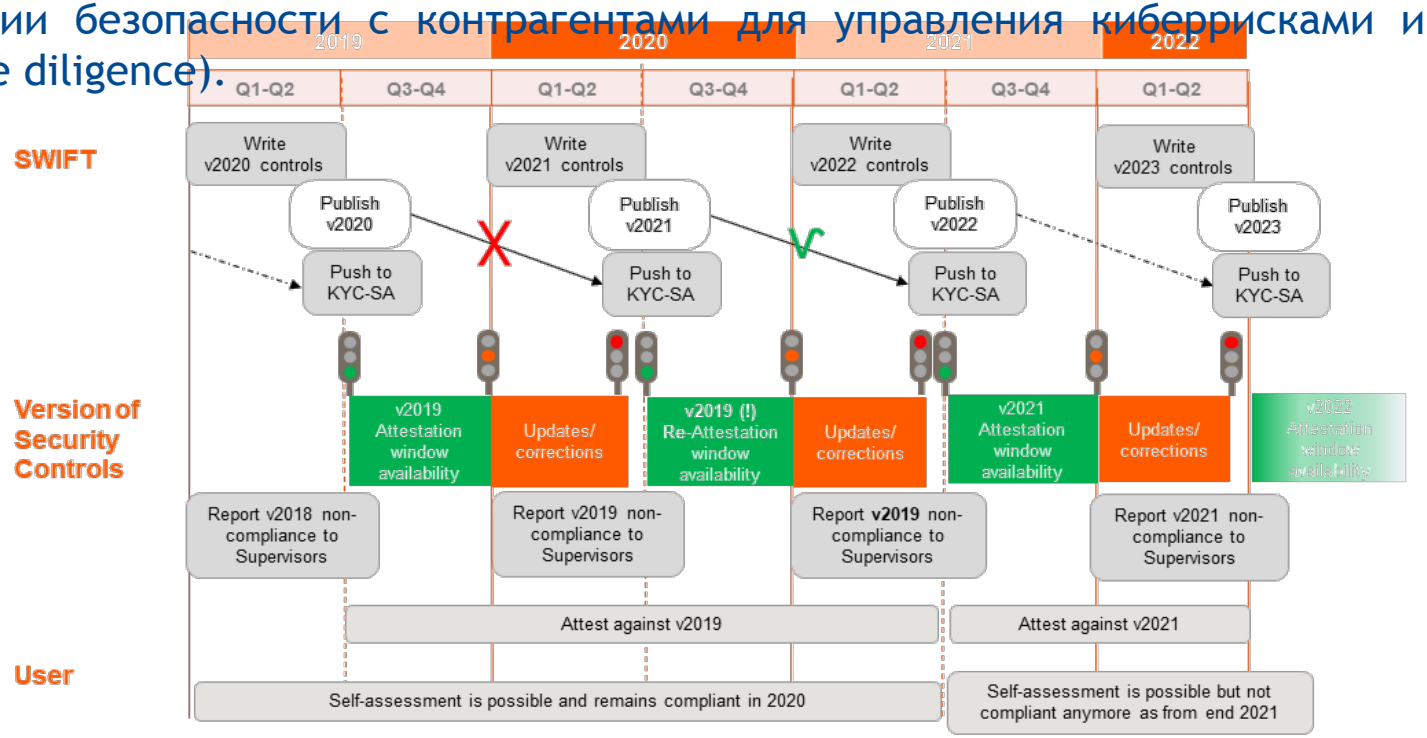
В ответ на атаки хакеров в 2017 году была разработана SWIFT Customer Security Programme (CSP)

Концепция обеспечения безопасности пользователей (CSCF) SWIFT состоит из 22 обязательных и 9 рекомендуемых мер защиты и элементов контроля (ЭК) для польз

Roadmap Customer Security Controls Framework

В начале альянс обязывал участников провести самоаттестацию по обязательным и, опционально, рекомендованным элементам контроля, а с середины 2020 года необходимо проводить независимую аттестацию на соответствие требованиям SWIFT CSCF (Customer Security Controls Framework).

Все результаты аттестации публикуются в KYC Registry (KYC-SA), которое является центральным приложением для пользователей , что способствует прозрачному обмену информацией о состоянии безопасности с контрагентами для управления киберрисками и оценки контрагентов (due diligence).



SWIFT CSCF 2021 vs NIST Cybersecurity Framework 1.1 vs ISO 27002 (2013) vs PCI DSS 3.2.1

Банкам легко включить SWIFT CSCF в действующую политику информационной безопасности, т.к. ее разработчики принимают во внимание здравый смысл и новейшие передовые практики и учитывают специфическую для пользователя инфраструктуру и конфигурации.

SWIFT CSCF 2021	Концепция кибербезопасности NIST версии v1.1	ISO 27002 (2013)	PCI DSS 3.2.1
1.1 Защита среды SWIFT Обеспечение защиты пользовательской локальной инфраструктуры SWIFT от потенциально скомпрометированных элементов общей ИТ-среды и внешней среды.	Управление доступом (PR.AC) PR.AC-5: защита целостности сети, включающая в себя разделение на подсети в тех случаях, когда это целесообразно	Управление безопасностью сети (13.1) 13.1.3: разделение на подсети	Требование 1. Установить и поддерживать конфигурацию брандмауэра для защиты данных владельца карты. Применяемые подразделы: 1.3
1.2 Контроль за привилегированными учетными записями операционной системы Ограничить и контролировать распределение и использование учетных записей операционной системы уровня администратора.	Управление доступом (PR.AC) PR.AC-4: управление правами на доступ с учетом принципов наименьших привилегий и разделения обязанностей.	Управление доступом пользователей (9.2) 9.2.3: управление правами привилегированного доступа.	Требование 8. Осуществлять идентификацию и аутентификацию доступа к компонентам системы. Применяемые подразделы: 8.1, 8.5

Обязательные и рекомендуемые элементы контроля CSCF 2021

1. Ограничение доступа в Интернет и защита наиболее важных систем от общей ИТ-среды

- 1.1 Обеспечение защиты среды SWIFT
- 1.2 Контроль за привилегированными учетными записями операционной системы
- 1.3 Защита платформы виртуализации
- 1.4 Ограничение доступа в Интернет

2. Уменьшение количества потенциальных векторов атак и уязвимостей

- 2.1 Защита внутреннего потока данных
- 2.2 Обновления системы безопасности
- 2.3 Повышение надежности системы
- 2.4A Безопасность потока данных бэк-офиса
- 2.5A Защита внешней передачи данных
- 2.6 Конфиденциальность и целостность сессии опера
- 2.7. Сканирование на уязвимость системы
- 2.8A Аутсорсинг критически важных видов деятельно
- 2.9A. Средства контроля транзакционного бизнеса
- 2.10 Повышение надежности приложений
- 2.11A Средства контроля RMA

3. Обеспечение физической безопасности среды

- 3.1 Физическая защита

Обязательные и рекомендуемые элементы контроля CSCF 2021 (продолжение)

4. Предотвращение компрометации учетных данных

- 4.1 Политика паролей
- 4.2 Многофакторная аутентификация

5 Управление идентификационными данными и разграничение полномочий

- 5.1 Логический контроль доступа
- 5.2 Управление токенами
- 5.3A Процесс проверки персонала
- 5.4. Физическое и логическое хранение паролей

6. Обнаружение аномальной активности в системах и журналах транзакций

- 6.1 Защита от вредоносных программ
- 6.2. Целостность программного обеспечения
- 6.3. Целостность базы данных17

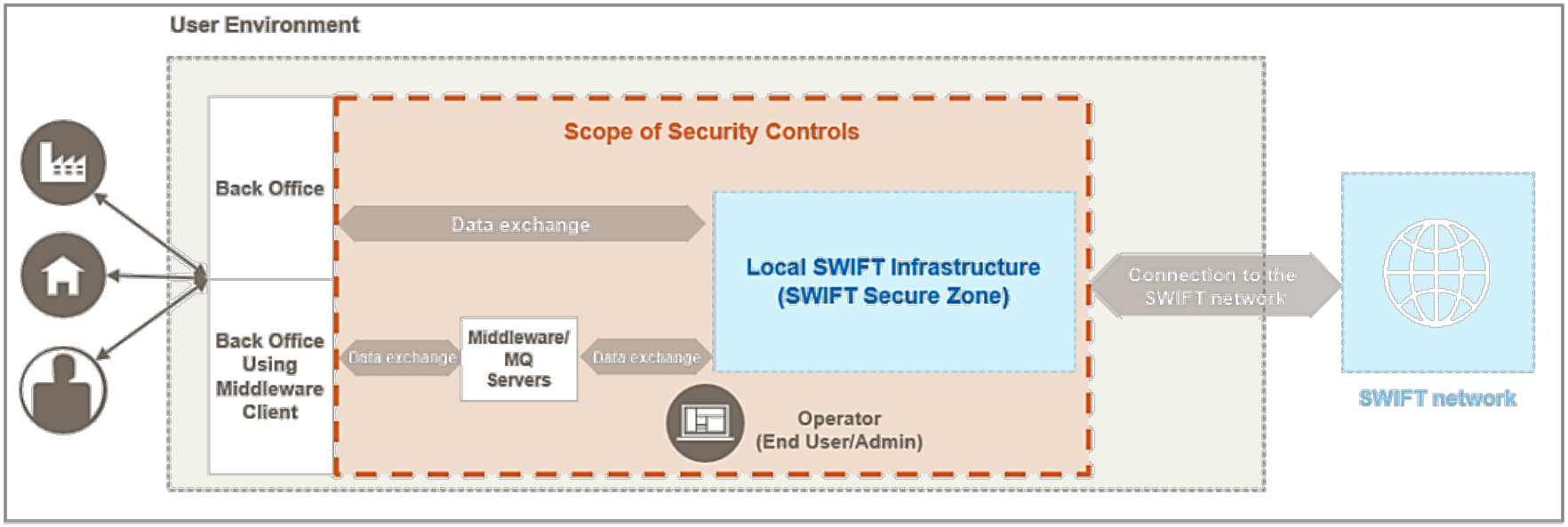
Подробное описание Сводная таблица по элементам контроля безопасности

- 6.4 Ведение журнала операций и мониторинг
- 6.5A Обнаружение вторжений

7. План реагирования на инциденты и информирование

- 7.1 Планирование реагирования на киберинциденты
- 7.2 Обучение и информирование в сфере безопасности
- 7.3A Тест на проникновение
- 7.4A Оценка рисков

Область применения SWIFT CSCF 2021

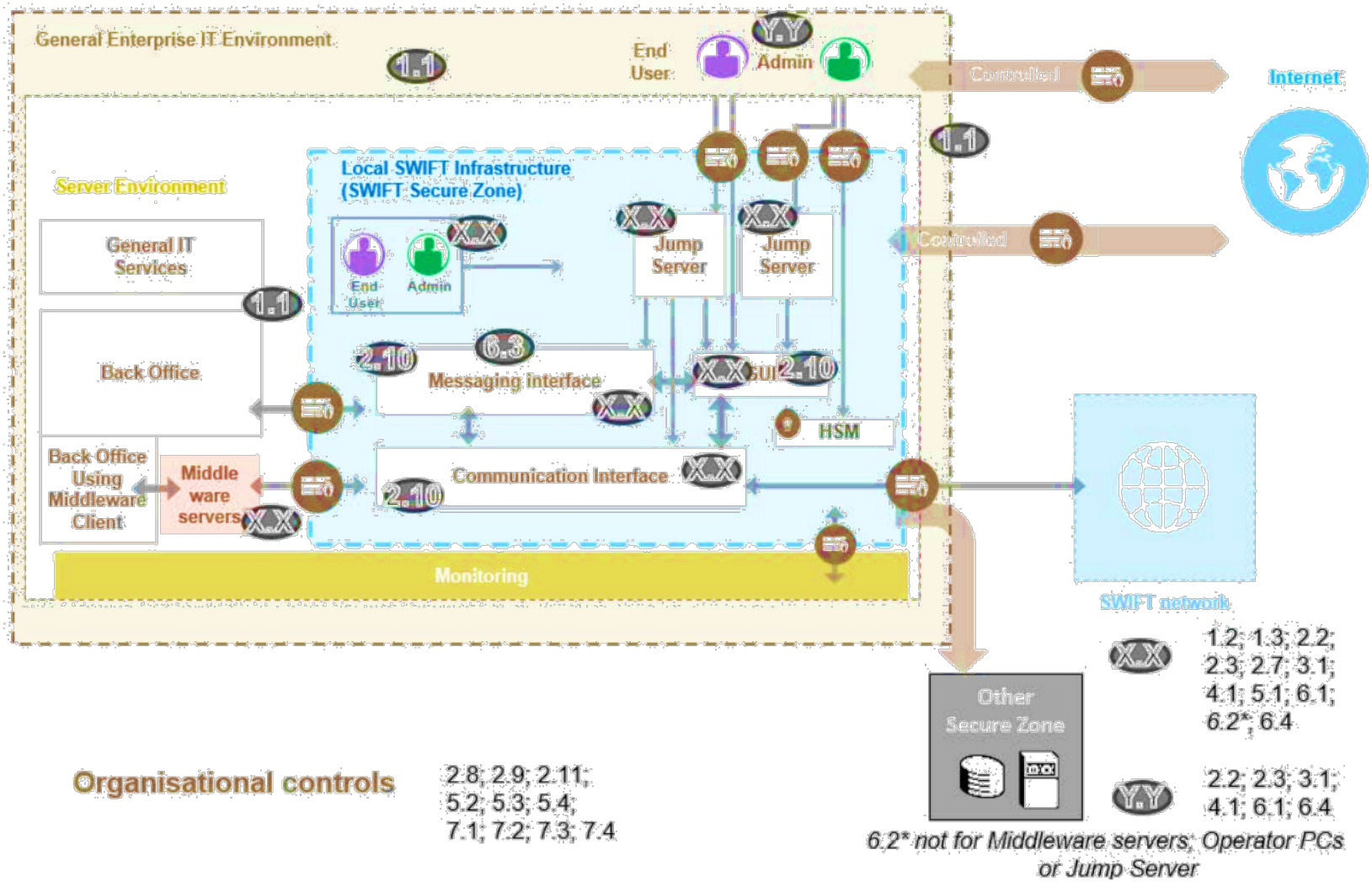


Зона безопасности содержит все компоненты локальной инфраструктуры SWIFT, но не ограничивается ими. Она включает в себя: интерфейс обмена сообщениями, коммуникационный
интерфейс, графический интерфейс на базе браузера, SWIFTNet Link, аппаратный модуль системы безопасности (HSM), коннектор SWIFT, промежуточный сервер и
любые применимые ПК оператора, предназначенные исключительно для работы или администрирования локальной инфраструктуры SWIFT.

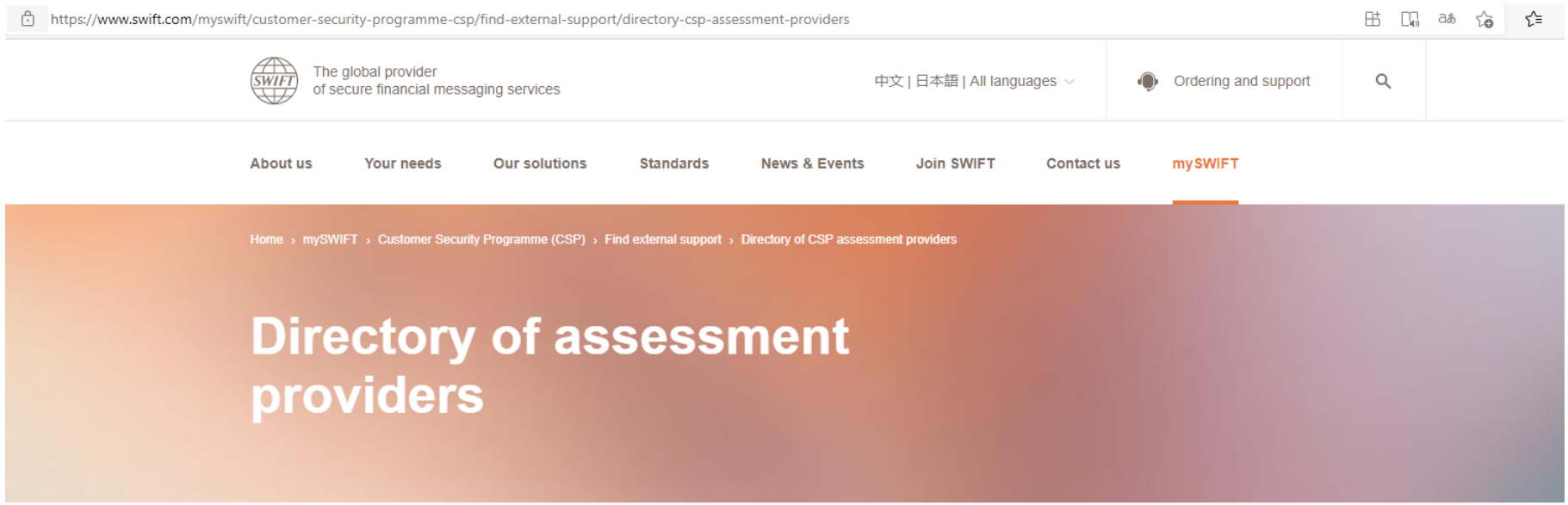
Основные моменты SWIFT CSCF 2021

1. Все компоненты SWIFT должны быть в отдельном физически от основной инфраструктуры Банка контуре безопасности (свои сервера и коммуникационное оборудование)
2. Брандмауэры транспортного уровня, создающие границу контура безопасности, должны быть физически или виртуально предназначены для защиты зоны безопасности.
3. Операторы/администраторы работают с компонентами SWIFT локально внутри контура безопасности
4. В случае удаленной работы операторов/администраторов должен использоваться jump-сервер
5. 2FA для операторов/администраторов
6. Физический доступ к серверам и др. оборудованию должен контролироваться и только для администраторов системы.
7. Желательно отделение от общих корпоративных ИТ-сервисов

Пример реализации



Выбор внешнего аудитора



Directory of CSP assessment providers

SWIFT has created a Directory of CSP assessment providers for your reference when looking for assessment providers in your country. These companies can help you to assess your level of compliance toward the implementation the CSP mandatory and advisory controls that apply to your connectivity configuration with SWIFT.

In listing firms in the Directory of CSP assessment providers, SWIFT has taken into account certain criteria, including:

- cyber security services experience & credentials
- strategic focus on cyber security services

Customer due diligence

You are responsible for completing your own due diligence when selecting and contracting CSP assessment providers or any other entity offering such services. You should, for instance, verify that individual consultants working for the selected provider:

- Have sufficient training and knowledge of SWIFT and SWIFT security – including understanding of the SWIFT security control framework and detailed mandatory and advisory controls
- Hold recognised industry qualifications: consultants should maintain industry recognised security qualifications or certifications such as QSA, CISSP, CISA, CISM, ISO, SANS.
- Are otherwise suitable for your needs and purposes

Отправка отчета

1-Зайти в приложение KYC-SA

Для заполнения результатов необходимы роли Предоставляющего (Submitter) – лицо, которое будет заполнять данные в приложение, и Утверждающего (Approver) – лицо, уполномоченное утвердить заполненную форму самоаттестации (директор по информационной безопасности – Chief Information Security Officer, CISO, или лицо с аналогичными функциями).

2-Заполнить черновик Аттестации

Заполнить опросник на основе полученного от Аудитора отчета

3-Завершить и отправить аттестацию

После заполнения черновика формы Аттестации назначенный Утверждающий (Approver) утвердит и направит на публикацию финальную версию аттестации. SWIFT проверит аттестацию на предмет указанной информации. После успешного завершения данной проверки статус Аттестации будет переведен в «опубликовано»

СПАСИБО ЗА ВНИМАНИЕ

АНДРЕЙ СТЕПАНОВ
Начальник Управления информационной безопасности Департамента по защите активов Банк СОЮЗ (АО)
Andrey.Stepanov@banksoyuz.ru