Управління безпекою

SWIFT випустив набір ключових стандартів з безпеки, які стануть обов'язковими для всіх користувачів SWIFT.

Застосування цих стандартів підвищить планку безпеки роботи користувачів у мережі SWIFT та подальшу підтримку користувачів у намаганнях щодо попередження та виявлення шахрайського використання їх інфраструктури. Впровадження цих стандартів також підвищить обізнаність та вправність у постійній боротьбі з кібер злочинністю пов’язаною із електронними переказами.

Ці ключові вимоги будуть застосовуватися до всіх користувачів SWIFT. Вони засновані на трьох цілях та восьми принципах, які наведені у таблиці нижче. 16 обов'язкових та 11 рекомендованих елементів контролю лежать в основі восьми принципів. Обов'язкові та рекомендовані елементи контролю також наведені нижче. Повна документація щодо елементів контролю буде доступна для ознайомлення до кінця жовтня з подальшим 2-місячним періодом її схвалення користувачами, починаючи з 1 листопада і до кінця року. SWIFT буде залучати до цього питання співтовариство та, зокрема, Національні Групи Членів протягом цього періоду для отримання зворотнього зв’язку. У 1 кварталі 2017 року будуть опубліковані остаточні описи елементів контролю.

Для того, щоб забезпечити їх використання, SWIFT вимагатиме від своїх користувачів запровадження детальної само-атестації щодо дотримання обов'язкових елементів контролю починаючи з 2-го кварталу 2017 року. Контроль за дотриманням обов'язкових вимог почнеться з січня 2018 року, включаючи перевірки внутрішніми та зовнішніми аудиторами вибіркових клієнтів з метою перевірки якості. Докладний статус відповідності вимогам кожного користувача буде доступний їхнім контрагентам (наприклад, через KYC Registry), забезпечуючи прозорість їхньої самостійної атестації та інспекцію результатів, дозволяючи іншим користувачам мережі оцінювати ризики при прийнятті рішень стосовно своїх відносин з контрагентами.

3 Цілі	**8 Принципів**	**27 Елементів контролю**
Убезпечте Ваше локальне середовище	1. Обмеження доступу до мережі інтернет 2. Відокремлення критичних систем від загального середовища IT 3. Зменшення поверхні для атак та вразливостей системи 4. Фізична безпека середовища	· Стосуються всіх користувачів та всього ланцюга проходження транзакції за межами локальної інфраструктури SWIFT · Відповідають міжнародно визнаним стандартам – NIST, PCI-DSS та ISO 27002

		· Деякі елементи контролю є обов’язковими, інші – рекомендовані · Документація та інші матеріали будуть доступні для ознайомлення до кінця жовтня
Знайте та Обмежуйте доступ	5. Запобігання компрометації облікових даних 6. Управління ідентифікаціями та розподілення адміністративних прав	
Виявляйте та Реагуйте	7. Виявлення підозрілої активності в системах або записах транзакцій 8. План Реагування на інцинденти та Обмін інформацією	

Обов’язкові елементи контролю

1. Обмеження доступу до мережі інтернет

2. Відокремлення критичних систем від загального середовища IT

M1.Управління адміністративним обліковим записом Операційної системи	**Свідчення контролю:** Доступ до локальних облікових записів операційної системи з правами адміністратора на рівні системи обмежені в максимально можливій мірі, використання контролюється, перевіряється та допускається тільки для здійснення відповідних заходів, таких як встановлення та налаштування програмного забезпечення, технічного обслуговування та надзвичайних дій. У всіх інших випадках, облікові записи обмежені для доступу.
M2. Виділення середовища SWIFT	**Свідчення контролю:** сегментована та захищена зона захищає середовище SWIFT від зламу та нападів з боку оточення, у якому існує підприємство, та зовнішнього середовища.

3. Зменшення видів атак та вразливостей системи

M3. Внутрішня безпека передачі даних	**Свідчення контролю:** механізми конфіденційності, цілісності та аутентифікації реалізовані для захисту передачі даних системи SWIFT між системами в межах безпечної зони інфраструктури, пов’язаної зі SWIFT, а також між комп'ютерами користувачів та безпечною зоною інфраструктури, пов’язаної зі SWIFT.

M4. Оновлення системи безпеки	**Свідчення контролю:** На всьому апаратному та програмному забезпеченні всередині безпечної зони інфраструктури, пов’язаної зі SWIFT, а також на комп’ютерах користувачів, що знаходяться в межах підтримки життєвого циклу постачальника, має бути встановлені обов'язкові оновлення програмного забезпечення, та оперативно встановлені оновлення системи безпеки.
M5. Покращення стабільності системи	**Свідчення контролю:** Посилення безпеки здійснено на всіх системах та інфраструктурі в межах безпечної зони інфраструктури, пов’язаної зі SWIFT, а також на комп'ютерах користувачів.

4. Фізична безпека середовища

M6. Фізична безпека	**Свідчення контролю:** Встановлено фізичний контроль засобів безпеки для захисту від несанкціонованого доступу до чутливого обладнання, системи хостингу сайтів та складських приміщень.

5. Запобігання компрометації облікових даних

M7. Використання паролів	**Свідчення контролю:** Всі паролі до облікових записів додатків та операційної системи повинні відповідати таким параметрам, як довжина, складність, обмеження невдалих спроб входу в систему.
M8. Багатофакторна аутентифікація	**Свідчення контролю:** Як мінімум – двофакторна аутентифікація має використовуватись для доступу до системи обміну повідомленнями SWIFT та комунікаційних додатків.

6. Управління ідентифікаціями та розподілення адміністративних прав

M9. Керування обліковими записами користувачів	**Свідчення контролю:** Облікові записи визначаються відповідно до принципів безпеки: доступ до даних за принципом «належить знати», з найменшими адміністративними правами, розподілом обов'язків.
M10. Керування токенами	**Свідчення контролю:** Токени аутентифікації управляються відповідним чином під час видачі, відкликання, використання та зберігання.

7. Виявлення підозрілої активності систем або у записах транзакцій

M11. Захист від шкідливих програм	**Свідчення контролю:** Програмне забезпечення для захисту від вірусів та шкідливих програм від авторитетного постачальника має бути встановлено та завжди підтримуватися оновленим до останніх версій на всіх системах.

M12. Цілісність бази даних	**Свідчення контролю:** Перевірка цілісності бази даних виконується програмними додатками в безпечній зоні інфраструктури, пов’язаної зі SWIFT, з регулярними інтервалами, встановленими в базах даних. Файли даних використовуються виключно для сервісів SWIFT.
M13. Ведення системного журналу та моніторинг	**Свідчення контролю:** Можливості для виявлення підозрілої активності реалізовані та встановлений процес або інструмент частої перевірки системних журналів.
M14. Цілісність програмного забезпечення	**Свідчення контролю:** Перевірка цілісності програмного забезпечення в програмних додатках в безпечній зоні інфраструктури, пов’язаної зі SWIFT, здійснюється при запуску та з регулярними інтервалами після цього.

8. План Реагування на інциденти та Обмін інформацією

M15. План реагування на кібер інциденти	**Свідчення контролю:** Організація має розроблений план реагування на кібер - інциденти.
M16. Навчання з питань безпеки та обізнаность	**Свідчення контролю:** Щорічні тренінги з питань безпеки проводяться для всіх співробітників, а тренінги щодо спеціальних ролей проводяться щорічно для осіб з адміністративними правами в системі SWIFT.

Поради щодо контролю безпеки

1. Обмеження доступу до мережі інтернет

2. Відокремлення критичних систем від загального середовища IT

3. Зменшення поверхні для атак та вразливостей системи

A1. Захист потоків даних бек-офісу	**Свідчення контролю:** механізми конфіденційності, цілісності та аутентифікації реалізовані для захисту передачі даних між системами бек-офісу та безпечною зоною інфраструктури, пов’язаної зі SWIFT.
A2. Захист зовнішньої передачі даних	**Свідчення контролю:** конфіденційні дані, що передаються з безпечної зони інфраструктури, пов’язаної зі SWIFT, повинні шифруватися.
A3. Надійність сеансу передачі даних	**Свідчення контролю:** надійність та конфіденційність інтерактивних сеансів передачі даних користувачів мають бути захищені.
A4. Сканування вразливостей	**Свідчення контролю:** сканування вразливостей виконується всередині безпечної зони інфраструктури, пов’язаної зі SWIFT, а також на комп'ютерах користувачів з використанням сучасних інструментів сканування, що відповідають галузевим стандартам.

A5. Аутсорсинг важливих видів операцій	**Свідчення контролю:** Будь-які важливі види операцій, що знаходяться на аутсорсингу, мають бути захищеними, як мінімум, на тому ж рівні, як і в самій організації.
A6. Елементи контролю бізнесу, пов'язаного з транзакціями	**Свідчення контролю:** Здійснення контролю, який обмежуватиме здійснення транзакцій в межах очікуваних транзакцій з відомими контрагентами.

4. Фізична безпека середовища

5. Запобігання компроментації облікових даних

6. Управління ідентифікаціями та розподілення адміністративних прав

A7. Процес перевірки персоналу	**Свідчення контролю:** Персонал, який працює з системою SWIFT перевіряється на надійність при призначенні на цю роль та періодично проходить перевірки.
A8. Фізичне та логічне зберігання паролів	**Свідчення контролю:** Будь-які записані паролі для адміністративних облікових записів, які використовуються в безпечній зоні інфраструктури пов'язаної зі SWIFT, зберігаються у фізично та логічно захищеному місці, з обмеженим доступом до даних за принципом «належить знати».

7. Виявлення підозрілої активності в системах або записах транзакцій

A9. Виявлення проникнення в локальну мережу	**Свідчення контролю:** Елементи контролю за виявленням проникнення повинні бути реалізовані для виявлення несанкціонованого доступу до мережі.

8. План Реагування на інциденти та Обмін інформацією

A10. Тестування на можливість проникнення	**Свідчення контролю:** Тестування на можливість проникнення в програмні додатки, головний сервер та в мережу здійснюється принаймні раз в рік всередині безпечної зони інфраструктури, пов'язаної зі SWIFT, а також на комп'ютерах користувачів.
A11. Аналіз ризику заснований на Сценаріях	**Свідчення контролю:** Проводиться оцінка ризиків на основі сценаріїв з використанням отриманих уроків для покращення реагування на інциденти та зміцнення можливостей захисту.