SGB Bank SA

DORA - projekt w Zrzeszeniu SGB

WDROŻENIE DORA

OBSZARY DORA

Zarządzanie Ryzykiem ICT

Plan ciągłości działania i plany awaryjne

Zarządzanie Incydentami

Proces cyberbezpieczeństwa i raportowania

Testowanie odporności cyfrowej

Testy penetracyjne systemów

Zarządzanie ryzykiem dostawców usług ICT

Ochrona przed atakami na łańcuchy dostaw i naruszeniami ze strony osób trzecich

Wymiana Informacji

Wymiana informacji o zagrożeniach

WDROŻENIE DORA

PUNKT STARTU

zgodnie z zasadą proporcjonalności …

USŁUGA ICT

[Art. 3] usługi cyfrowe i usługi w zakresie danych świadczone w sposób ciągły za pośrednictwem systemów ICT na rzecz co najmniej jednego użytkownika wewnętrznego lub zewnętrznego, łącznie ze sprzętem komputerowym jako usługą i usługami w zakresie sprzętu komputerowego obejmującymi zapewnianie wsparcia technicznego za pośrednictwem aktualizacji oprogramowania lub oprogramowania układowego przez dostawcę sprzętu, z wyłączeniem tradycyjnych usług telefonii analogowej; [Preambuła] definicję (…) należy rozumieć szeroko (…)

FUNKCJA KRYTYCZNA lub ISTOTNA

[Art. 3] funkcja, której zakłócenie w sposób istotny wpłynęłoby na wyniki finansowe podmiotu finansowego, na bezpieczeństwo lub ciągłość usług i działalności tego podmiotu lub której zaprzestanie lub wadliwe lub zakończone niepowodzeniem działanie w sposób istotny wpłynęłoby na dalsze wypełnianie przez podmiot finansowy warunków i obowiązków wynikających z udzielonego mu zezwolenia lub jego innych obowiązków wynikających z obowiązujących przepisów dotyczących usług finansowych

WDROŻENIE DORA

RAMY ZARZĄDZANIA RYZYKIEM ICT

Strategia operacyjnej odporności cyfrowej – określająca sposób wdrażania ram, zawierająca takie elementy, jak: limit tolerancji ryzyka, kluczowe wskaźniki ryzyka, architekturę ICT, mechanizmy zarządzania incydentami, strategię komunikacji, testowanie operacyjnej odporności cyfrowej, powiązanie zarządzania ryzykiem z celami biznesowymi

Dokumentacja funkcji biznesowych wspieranych przez ICT

Polityka bezpieczeństwa informacji

Polityka dot. kryptografii i metod uwierzytelniania

Polityka dot. poprawek i aktualizacji

Polityka dot. uprawnień dostępu (fizyczny i logiczny)

Polityka dot. zarządzania zmianą w systemach ICT

Polityka tworzenia kopii zapasowych i przywracania danych

Procedury dot. wykrywania, obsługi i reagowania na wystąpienie incydentów

Program testowania operacyjnej odporności cyfrowej (metodyki, narzędzia, testy, w tym: bezpieczeństwa, podatności, wydajności)

Rejestr ustaleń umownych

Strategia na rzecz ciągłości działania (w tym polityka komunikacji)

Strategia zarządzania ryzkiem dot. zewnętrznych dostawców usług ICT

WDROŻENIE DORA

AKTY TOWARZYSZĄCE: w konsultacji

publikacja ostatecznych wersji: do 17 stycznia 2024 r.

REGULACYJNE I WYKONAWCZE STANDARDY TECHNICZNE

Obszar	Delegacja
RTS Zarządzanie ryzykiem ICT	art. 15, 16
RTS Kryteria klasyfikacji incydentów ICT	art. 18
ITS Wzory i rejestrów i informacji	art. 28
RTS Usługi ICT świadczone przez dostawców	art. 28

WDROŻENIE DORA

AKTY TOWARZYSZĄCE: w konsultacji

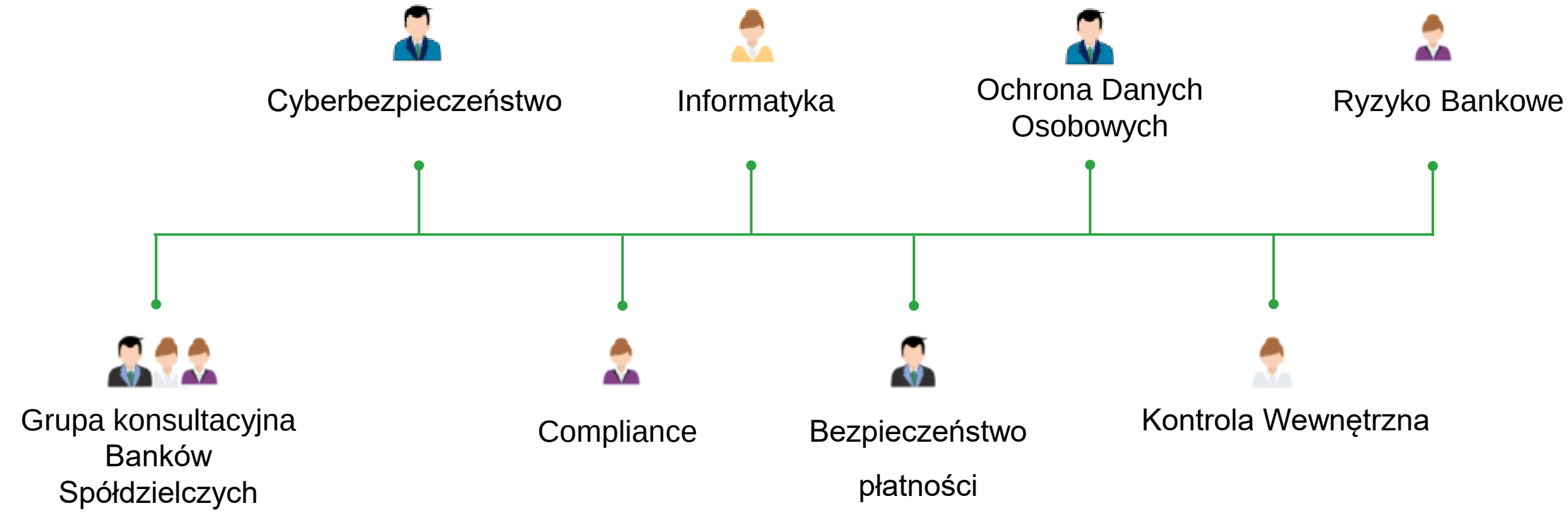
publikacja ostatecznych wersji: do 17 lipca 2024 r.

REGULACYJNE I WYKONAWCZE STANDARDY TECHNICZNE

Obszar	Delegacja
RTS Zgłaszanie poważnych incydentów	art. 20
RTS Testy penetracyjne	art. 26
ITS Wzory i procedury zgłaszania poważnych incydentów	art. 20
RTS Zlecanie usług ICT wspierających funkcje krytyczne lub istotne	art. 30

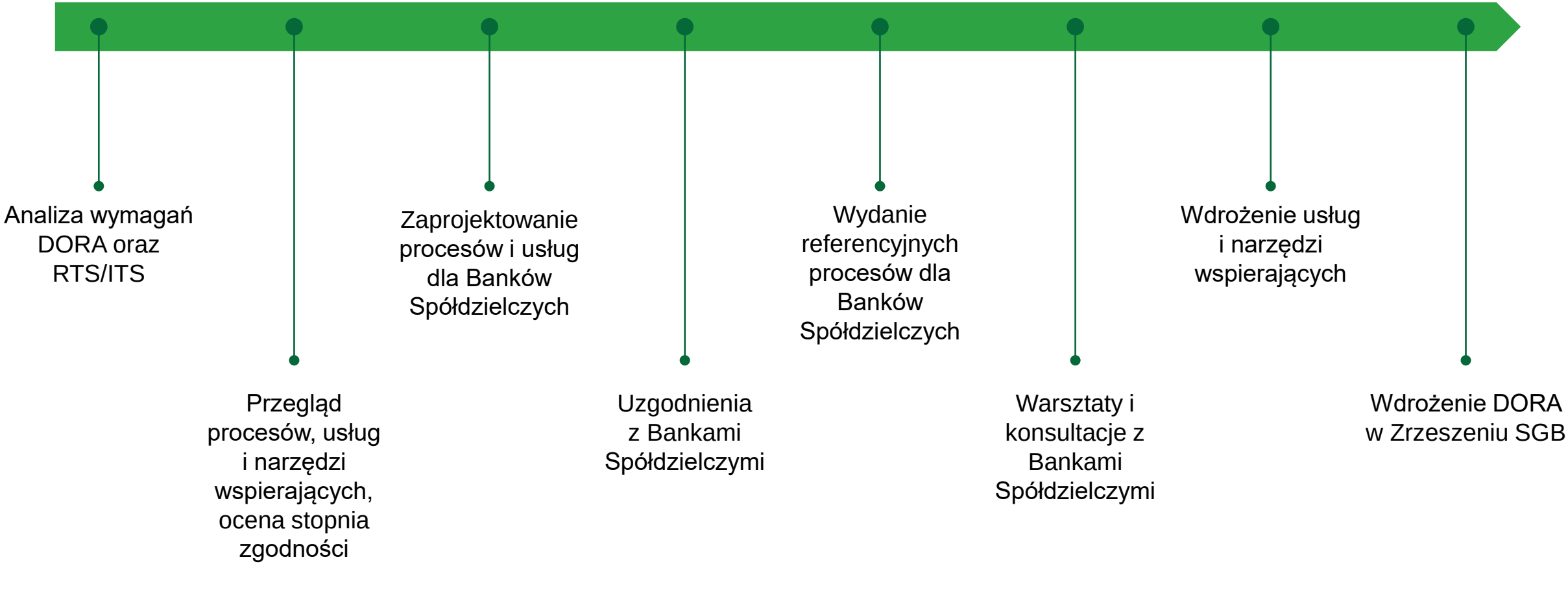
WDROŻENIE DORA

ZESPÓŁ PROJEKTOWY SGB



WDROŻENIE DORA

RAMOWY PLAN DZIAŁAŃ



WDROŻENIE DORA

PROCESY WYMAGAJĄCE PRZEGLĄDU i AKTUALIZACJI

- Strategia zarządzania ryzykiem
- Strategia w zakresie obszarów technologii informacyjnej oraz bezpieczeństwa IT
- Zasady zarządzania ryzykiem IT
- Polityka bezpieczeństwa informacji
- Polityka ciągłości działania
- Regulamin zarządzania projektami
- Regulamin zarządzania incydentami IT
- Regulamin zarządzania zmianami IT
- Regulamin testowania oprogramowania
- Procedura zakupów
- Polityka powierzania wykonywania czynności podmiotom zewnętrznym
- Regulamin funkcji kontroli
- Instrukcja opiniowania umów

SGB

OTWIERAMY PRZYSZŁOŚĆ

- DOBRO KLIENTA
- DOBRO GRUPY
- CYFROWA MOC
- EFEKTYWNOŚĆ
- PRACOWNICY
- LOKALNOŚĆ