Wyzwania bankowości – cyberbezpieczeństwo i compliance

Raiffeisen POLBANK

Piotr Czarnecki
Prezes Zarządu
Raiffeisen Bank Polska S.A.

Cyberbezpieczeństwo

Raiffeisen POLBANK

Cyberbezpieczeństwo jako jeden z najważniejszych aspektów prowadzenia współczesnego biznesu

- Powszechność i zakres zastosowania rozwiązań IT - uzależnienie funkcjonowania przedsiębiorstw od systemów informatycznych.
- Bezpieczeństwo biznesu - nie tylko kwestia ciągłości operacyjnej.
- Cyberprzestępstwa – najszybciej rosnące źródło ryzyka biznesowego.
- Od czego zależy poziom bezpieczeństwa przedsiębiorstw?

Stare zagrożenia w nowych odsłonach

- Socjotechniki
- Szkodliwe oprogramowanie (malware)
- Podatności w systemach, w tym podatności *0-day*
- Wycieki danych
- Ataki DDoS
- Ataki skierowane na użytkowników internetowych systemów transakcyjnych i wykorzystywane przez nich komputery.

Nowe zagrożenia

- Ataki ukierunkowane (z wykorzystaniem szkodliwego oprogramowania *APT* i *AVT*)
- Ataki na urządzenia *IoT* (samochody, urządzenia AGD) oraz ataki skierowane na luki w oprogramowaniu sprzętowym (*firmware*) różnych urządzeń (nie tylko komputerowych)
- Ataki na urządzenia mobilne
- Ataki na systemy przemysłowe (sterowanie SCADA)
- Ataki na systemy rozproszone w chmurze obliczeniowej
- Ataki na urządzenia medyczne
- Ataki na systemy monitoringu i sterowania inteligentnymi budynkami
- Ataki na środowiska i systemy wirtualne
- Ataki wielowektorowe i wielowątkowe o skomplikowanym przebiegu i wielu celach

Zagrożenia – wczoraj i dziś

Współcześnie realizowane persystentne ataki sprofilowane na przedsiębiorstwa pozostają niewykrywalne dla tradycyjnych, punktowo działających systemów bezpieczeństwa, co sprawia, że są one i pozostaną prawdziwym wyzwaniem dla służb bezpieczeństwa IT w każdym przedsiębiorstwie.

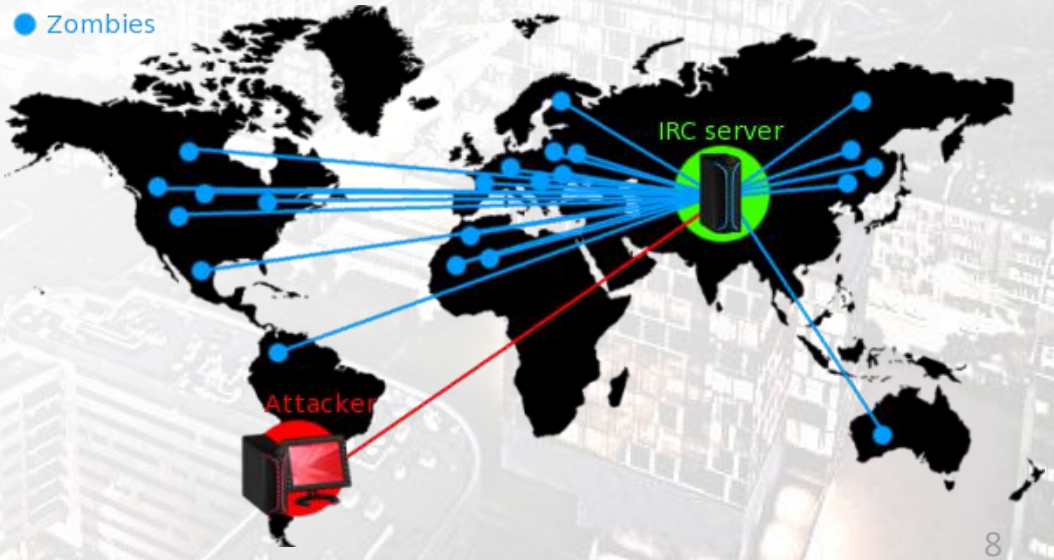
Najważniejsze wyzwania

- Zapewnienie odpowiedniego budżetu na bezpieczeństwo.
- Umocowanie jednostek organizacyjnych zajmujących się zapewnieniem bezpieczeństwa w przedsiębiorstwach wystarczająco wysoko w strukturach zarządczych, by zapewnić im decyzyjność i egzekwowalność decyzji.
- Rekrutacja na deficytowym rynku ekspertów zajmujących się cyberbezpieczeństwem.

- Zapewnienie odpowiedniej jakości kooperacji poszczególnych podmiotów odpowiedzialnych za bezpieczeństwo, w tym jednostek biznesowych, IT i jednostek zajmujących się bezpieczeństwem informacji.
- Edukacja dla bezpieczeństwa i kształtowanie świadomości w tym zakresie wśród kierownictwa wszystkich – bez wyjątków - szczebli, pracowników oraz klientów.

Najważniejsze wyzwania

- Stały monitoring rodzaju i stanu zagrożeń oraz wynikającego z nich ryzyka dla przedsiębiorstwa, a także – w ślad za tym – wdrażanie możliwie najskuteczniejszych i jednocześnie uzasadnionych ekonomicznie rozwiązań dla zapewnienia bezpieczeństwa – zarówno proceduralno-organizacyjnych jak i technicznych.
- Zapewnienie bezpieczeństwa w projektach informatycznych, by bezpieczeństwo było wbudowane w tworzone w przedsiębiorstwie rozwiązania informatyczne w pełnym cyklu ich rozwoju.
- Zapewnienie wysokiej jakości zarządzania podatnościami, aktualizacjami i poprawkami bezpieczeństwa w celu jak najwcześniejszego wykrywania i korygowania podatności w systemach przedsiębiorstwa.



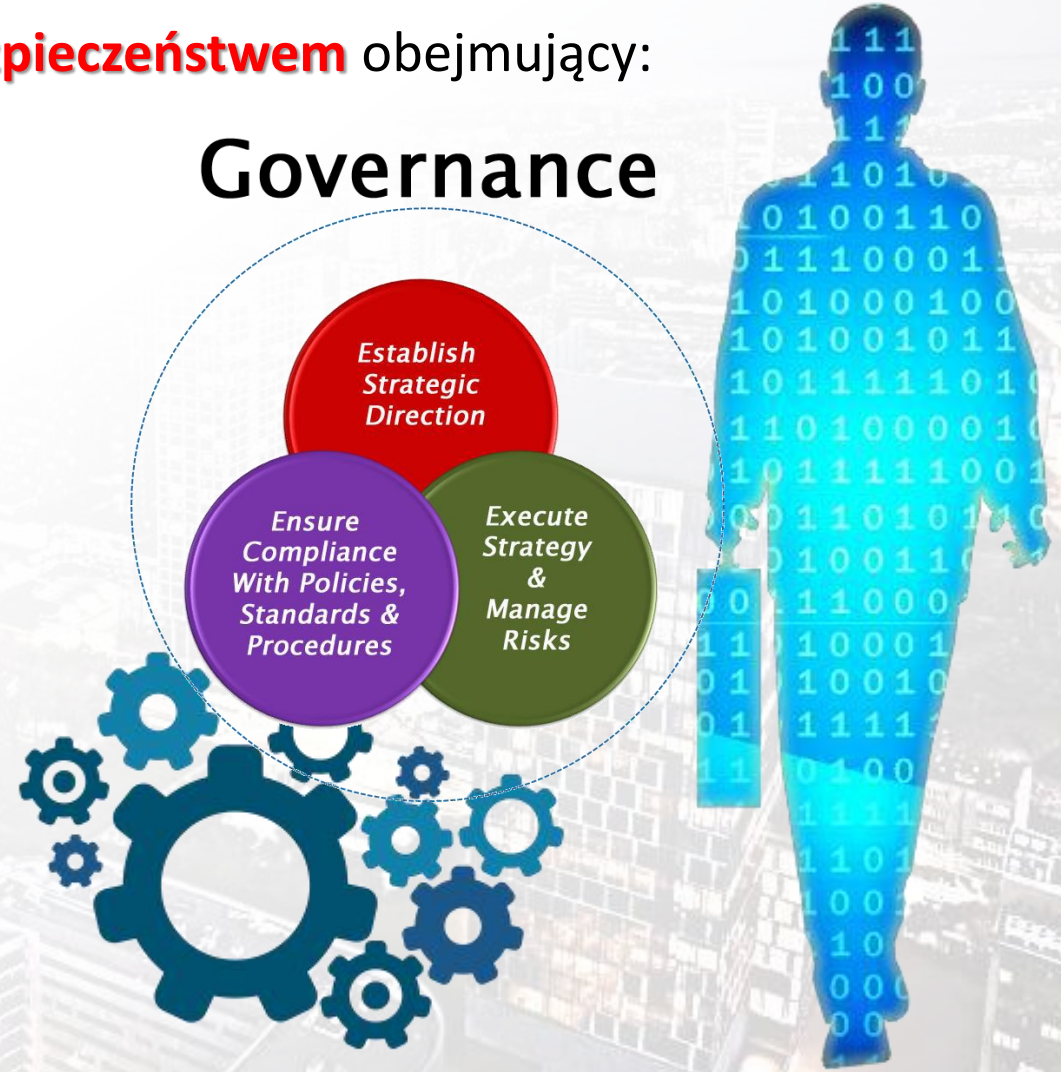
Najważniejsze wyzwania

- Zapewnienie ochrony przed sprofilowanymi atakami i szkodliwym oprogramowaniem typu APT i AVT.
- Kompleksowe zarządzanie zdarzeniami i incydentami bezpieczeństwa w trybie ciągłym przez wyspecjalizowane zespoły reagowania na incydenty i centra operacyjne bezpieczeństwa (SOC). Detekcja zdarzeń mających istotny wpływ na bezpieczeństwo przedsiębiorstw w oparciu o logikę korelacyjną systemów klasy SIEM.

Co decyduje o cyberbezpieczeństwie banków?

Zintegrowany system zarządzania bezpieczeństwem obejmujący:

- Standardy bezpieczeństwa
- Systemy bezpieczeństwa
- Procesy
- Ludzie i ład organizacyjny



Gdzie i jak materializują się obecnie najpoważniejsze cyber-zagrożenia w sektorze bankowym?

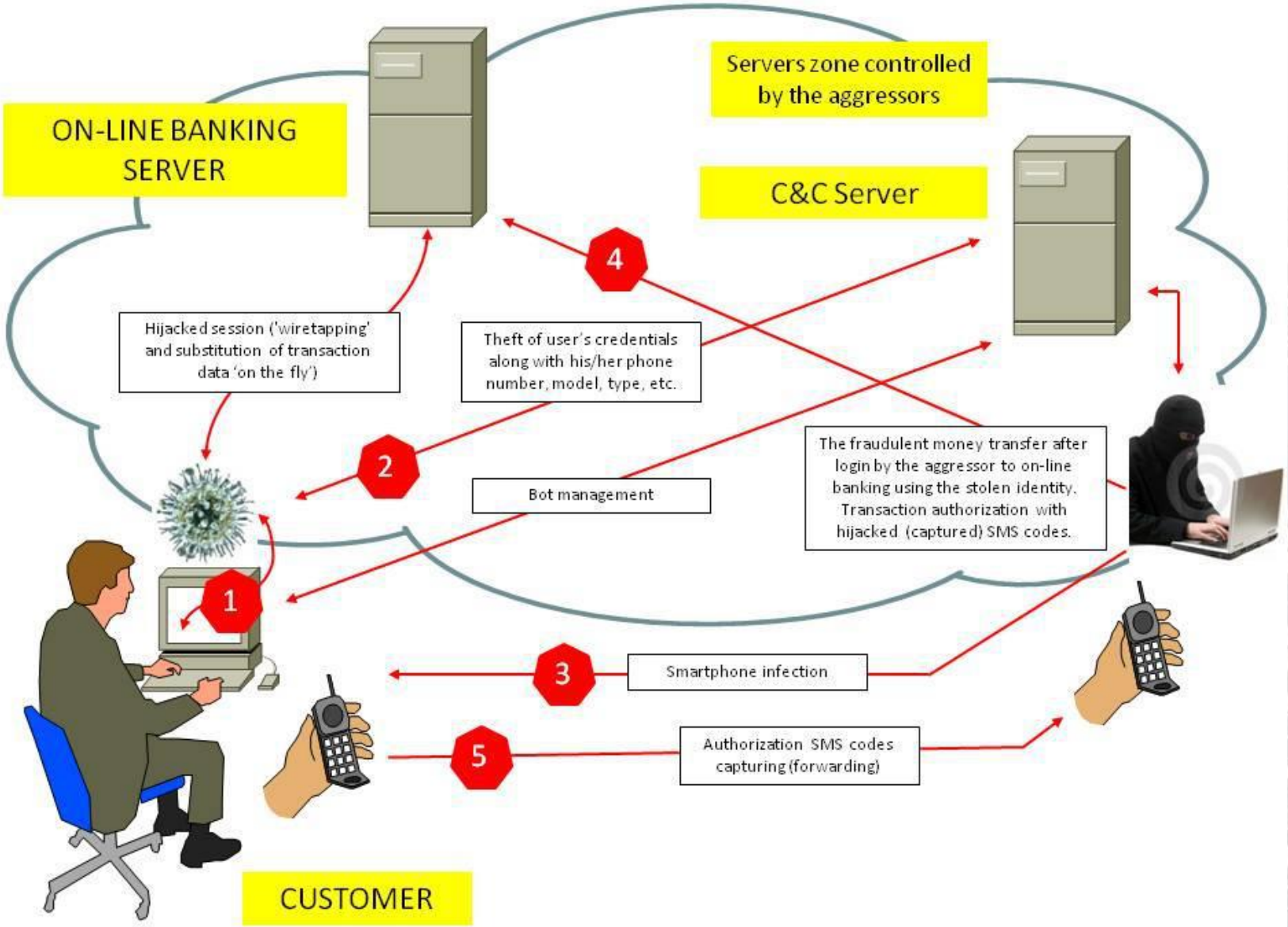
- Zagrożenia po stronie operatora internetowego systemu transakcyjnego i jego infrastruktury (banku)
- Zagrożenia po stronie sieci
- Zagrożenia po stronie klienta

Mówiąc o cyberbezpieczeństwie, co właściwie mamy na myśli?

- Czym jest luka w bezpieczeństwie?
- Co to jest wytrych?
- Czym jest wektor ataku?
- Jak dochodzi do „włamania”?
- Rola socjotechnik w przepisie na udany atak

Raiffeisen POLBANK

Jak wygląda mechanizm internetowego oszustwa, którego celem jest klient banku?



Jak się nie dać?

Perspektywa klienta:

- Przestrzeganie zasad bezpieczeństwa.
- Uodpornienie na socjotechniczne „sztuczki” intruzów poprzez „szczepionkę” w postaci silnej dawki wiedzy o bezpieczeństwie, nie tylko użytkowania systemu transakcyjnego przez Internet, ale generalnie o bezpiecznym poruszaniu się po zasobach Internetu.

Perspektywa operatora systemu transakcyjnego (banku):

- Trzymać rękę na pulsie – śledzić zagrożenia i reagować na zmieniające się warunki.
- Wzmocnić proces wieloaspektowej autoryzacji operacji.
- Zastosować ochronę *anti-APT* w systemach organizacji
- Uczynić kontrolę *anti-DDoS* maksymalnie efektywną nawet w sytuacjach potężnych ataków tego typu.
- Wdrożyć system wczesnego reagowania na zagrożenia po stronie klienta.
- Wzmocnić zewnętrzny *security incident handling* oraz wymianę informacji o zagrożeniach z innymi organizacjami.
- Współpraca z organami ścigania i wymiaru sprawiedliwości.
- Działania edukacyjne i budujące świadomość bezpieczeństwa skierowane do klienta.
- Publikacje prasowe i wypowiedzi w mediach na temat bezpieczeństwa.


Compliance
Raiffeisen
POLBANK

Zmiany warunków prowadzenia biznesu, tendencje w regulowaniu działalności

Oczekiwania wobec Compliance

Rosnąca liczba organów regulujących działalność banków
(KNF, BFG, UOKiK, GIODO, GIIF, Rzecznik Finansowy, EBA, ESMA, BCBS).

Rosnąca liczba regulacji i obszarów regulowanych w działalności banków
(np. FATCA, MIFID2, CRS, CRD IV/CRR, MAD/MAR, EMIR, UCITS, AIFMD, wytyczne EBA dot. wynagrodzeń, ustawa o rozpatrywaniu reklamacji przez podmioty rynku finansowego (…), ustawa o działalności ubezpieczeniowej, ustawa o Bankowym Funduszu Gwarancyjnym, rekomendacje KNF (np. Rekomendacja U dot. bancassurance, projekt Rekomendacji Z dot. ładu korporacyjnego itd.), wytyczne KNF odnośnie oferowania produktów na rynkach OTC itd.

Zwiększanie obciążeń finansowych
(np. zwiększenie składek na BFG, domiary kapitałowe, podatek bankowy, „ustawa frankowa").

Konieczność zwiększania wewnętrznej efektywności kosztowej
(redukcje zatrudnienia, ograniczanie środków na szkolenia itp.).

Wpływ potrzeb finansowych podmiotów dominujących

Ewolucja podejścia do koncepcji *compliance* w ujęciu regulacyjnym

Nowe uregulowania prawne - zmiana pozycji funkcji *compliance* w bankach

Prawo bankowe (obow. od 2015)

- wyodrębnienie „komórki do spraw zgodności" w ramach II linii obrony systemu kontroli wewnętrznej i przydzielenie jej odpowiedzialności za zarządzanie ryzykiem braku zgodności

Rozp. Min. Fin. w sprawie systemu zarządzania ryzykiem i systemu kontroli wewn. (…) (od 01.01.2017?)

- mechanizmy zapewniające niezależność komórki ds. zgodności
- zapewnienie efektywności działania komórki

Rekomendacja H (od VII.2017?)

- uszczegółowienie postanowień RMF, głównie w zakresie operacyjnych oczekiwań odnośnie procesu zarządzania ryzykiem braku zgodności

Polska 2017 - nowa rola *compliance*

Rozwiązania wg projektu RMF ws. systemu zarządzania ryzykiem i systemu kontroli wewnętrznej (…), zastępującego uchwałę KNF nr

NIEZALEŻNOŚĆ

- **zakaz łączenia** z innymi komórkami i funkcjami,
- obligatoryjny **udział w posiedzeniach zarządu,**
- obligatoryjny **udział w posiedzeniach rady nadzorczej,** jeśli dotyczy systemu kontroli wewnętrznej,
- **ochrona pracowników** komórki ds. zgodności przed nieuzasadnionym wypowiedzeniem stosunku pracy,
- **kontrola wynagrodzeń** pracowników komórki ds. zgodności (zapewnienie obiektywizmu),
- bezpośredni **kontakt z zarządem, radą nadzorczą i komitetem audytu,**
- **obowiązek bezpośredniego i jednoczesnego raportowania** do zarządu i rady nadzorczej,
- powołanie i odwołanie kierującego komórką ds. zgodności wymaga **zgody rady nadzorczej i poinformowania KNF** z podaniem uzasadnienia.

EFEKTYWNOŚĆ

- pracownicy komórki ds. zgodności mają **dostęp do wszelkich informacji i dokumentów,** w tym poufnych,
- odpowiedzialność zarządu za **zapewnienie środków finansowych** niezbędnych do systematycznego podnoszenia umiejętności i kwalifikacji pracowników komórki ds. zgodności,
- zarząd podejmuje działania zapewniające **właściwą współpracę** wszystkich pracowników z komórką ds. zgodności.

ODPOWIEDZIALNOŚĆ

- **identyfikowanie** ryzyka braku zgodności, w szczególności poprzez analizę przepisów prawa, regulacji wewnętrznych banku, standardów rynkowych oraz przeprowadzanie wewnętrznych postępowań wyjaśniających,
- **ocenianie** ryzyka braku zgodności,
- **kontrola** ryzyka braku zgodności - stosowanie, bazujących na ocenie ryzyka braku zgodności, mechanizmów kontrolnych,
- **monitorowanie** poziomu ryzyka braku zgodności po zastosowaniu mechanizmów kontrolnych, w szczególności poprzez przeprowadzanie testów pionowych i weryfikacji bieżących,
- okresowe **raportowanie** w zakresie ryzyka braku zgodności do zarządu, rady nadzorczej i komitetu audytu.

Zmiana odpowiedzialności w systemie kontroli wewnętrznej?

Projekt Rekomendacji H w sprawie systemu kontroli wewnętrznej

AUDYT WEWNĘTRZNY

OCENA ADEKWATNOŚCI I SKUTECZNOŚCI SYSTEMU ZARZĄDZANIA,
DZIAŁALNOŚĆ DORADCZA

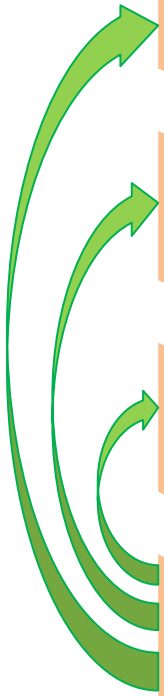
COMPLIANCE

ZARZĄDZANIE RYZYKIEM BRAKU ZGODNOŚCI
(W TYM STOSOWANIE MECHANIZMÓW KONTROLI RYZYKA, TESTOWANIE PIONOWE I WERYFIKACJE BIEŻĄCE PIONOWE)

FUNKCJA KONTROLI (WSZYSTKIE JEDNOSTKI BANKU)

ZAPEWNIANIE ZGODNOŚCI

Zasady zarządzania ryzykiem braku zgodności określone w przepisach prawa



IDENTYFIKACJA	Analiza przepisów, regulacji wewnętrznych, standardów rynkowych, wyników postępowań wyjaśniających, raportów i rejestrów wewn. zgłoszeń whistleblowing, monitorowanie otoczenia, udział w projektach…
OCENA	Modele oceny ryzyka braku zgodności, metody jakościowe (eksperckie) oceny ryzyka, mapy ryzyka, analizy scenariuszowe, profile ryzyka, odstępstwa, KRI/KPI itp.
KONTROLA	Projektowanie i implementacja mechanizmów kontrolnych (podział obowiązków, autoryzacje, weryfikacje, szkolenia, nadzór przełożonego itp.).
MONITOROWANIE	Weryfikowanie skuteczności mechanizmów kontrolnych (testowania pionowe, weryfikacje bieżące), ankiety, monitorowanie realizacji zaleceń, monitorowanie trendów (np. wzrost/spadek reklamacji itp.).
RAPORTOWANIE	Bieżące wskazywanie zidentyfikowanego ryzyka braku zgodności. Raportowanie okresowe i roczne dla komitetów, zarządu, rady nadzorczej. Udział w posiedzeniach zarządu, rady nadzorczej i komitetów.

Compliance w systemie nadzoru nad działalnością banku

Dziękuję za uwagę

Raiffeisen POLBANK