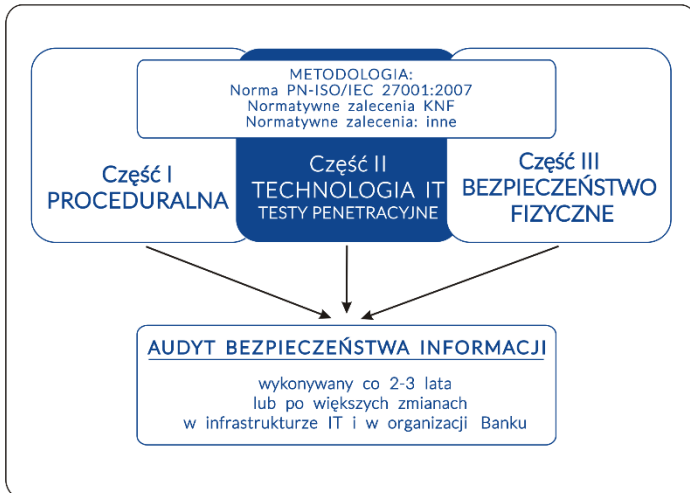


Szanowni Państwo,

Servus Comp Data Security przypomina o obowiązku realizacji założeń Komisji Nadzoru Finansowego, zgodnie z którymi każdy Bank Spółdzielczy zobligowany jest do przeprowadzenia raz na 2 - 3 lata lub po znaczących zmianach w infrastrukturze IT pełnego, zewnętrznego Audytu Bezpieczeństwa Informacji.



Zakres wymaganego audytu obejmuje:

- polityka bezpieczeństwa
- zgodność z wymaganiami prawnymi, KNF i własnymi standardami
- organizacja bezpieczeństwa informacji
- zarządzanie incydentami związanymi z bezpieczeństwem informacji
- zarządzanie ciągłością działania
- bezpieczeństwo zasobów ludzkich
- kontrola dostępu
- pozyskiwanie, rozwój i utrzymanie systemów informatycznych
- zarządzanie aktywami infrastruktury IT
- zarządzanie systemami i sieciami
- bezpieczeństwo fizyczne i środowiskowe.

W czasie audytu bardzo wnikliwie weryfikowane jest bezpieczeństwo proceduralne i informatyczne, przeprowadzane są również testy oprogramowania systemowego oraz infrastruktury informatycznej. Do testów penetracyjnych używane jest profesjonalne oprogramowanie, które gwarantuje identyfikację wszystkich potencjalnych zagrożeń dla środowiska informatycznego Banku.

Wynikiem audytu jest **poufny raport** identyfikujący zagrożenia w dotychczas funkcjonującym systemie bezpieczeństwa. Raport zawiera również rekomendacje audytorów w zakresie rozwiązań mających zapewnić bezpieczeństwo IT oraz zalecenia dotyczące procedur i dokumentacji.

Bank otrzymuje dokładny opis problemu i sugerowane rozwiązanie, jakie należy wdrożyć, aby zniwelować występujący problem.

Audyty wykonuje zespół doświadczonych audytorów posiadających Certyfikaty Audytora Wiodącego Systemu Zarządzania Bezpieczeństwem Informacji wg ISO/IEC 27001, certyfikaty ITIL Foundation. Zespół Audytorów zaznajomiony jest dokładnie z niuansami i specyfiką Banków Spółdzielczych i systemów Bankowych: NOVUM, SoftNet i Asecco defBank.

Ocena przeprowadzona zostanie zgodnie z wymaganiami prawnymi i normami w zakresie bezpieczeństwa informacji normy ISO 27001 oraz dobrych praktyk wynikających z metodyki COBIT (Control Objectives for Information and related Technology), które są wykorzystywane przez audytorów systemów informatycznych.

Po wykonanym Audycie Bank może wykorzystać wiedzę audytorów w razie wątpliwości w kwestii omawianych zagadnień.

Zalecamy pilny kontakt w celu weryfikacji niejasności oraz ustalenia terminu audytu:

Barbara Dyka **Servus Comp**
Koordynator ds. Audytów i Szkoleń
certyfikat ITIL Foundation
kom: 608 407 668 tel: +48 12 631 91 22
barbara.dyka@servus-comp.pl

Andrzej Popiołek **Servus Comp**
Audytor Wiodący SZBI, Szef Zespołu Audytorów, Audytor
Bezpieczeństwa Fizycznego, Infrastruktura Informatyczna
certyfikat ITIL Foundation
+48 602 220 749
andrzej.popiolek@servus-comp.pl