# AUDYT BEZPIECZEŃSTWA INFORMACJI

## KTO POWINIEN WYKONYWAĆ AUDYT BEZPIECZEŃSTWA INFORMACJI?

- ORGANY PAŃSTWOWE ROZLICZANE Z WYTYCZNYCH KRI – KRAJOWYCH RAM INTEROPERACYJNOŚCI
- FIRMY BIZNESOWE, W KTÓRYCH PRZYKŁADA SIĘ ZNACZĄCĄ WAGĘ DO BEZPIECZEŃSTWA INFORMACJI - CYBERBEZPIECZEŃSTWA
- Firmy posiadające certyfikację norm

**Audyt bezpieczeństwa informacji** stanowi niezależną ocenę aktualnie działającego systemu informatycznego w instytucji państwowej w firmie biznesowej wraz z jego infrastrukturą sprzętową, systemową i sieciową.

Oferujemy współpracę, w ramach której nasi eksperci przeprowadzą ocenę aspektów prawnych, organizacyjnych, technicznych i informatycznych. Wykonanie audytu pozwala zweryfikować stan systemu informatycznego i prawidłowość procedur zarządzania systemami IT wraz z poziomem ich zgodności z obowiązującymi normami i standardami. Realizowane przez nas działania audytowe są zgodne z wytycznymi KRI oraz wskazaniami normy ISO/IEC 27001 i przeprowadzane w odniesieniu do obiektywnych uwarunkowań i specyfiki danej organizacji, obowiązujących przepisów prawa i aktualnego stanu technologii.

Zgodnie ze standardem Systemu Zarządzania Bezpieczeństwem Informacji w ramach obowiązującej normy ISO/IEC 27001 nasi eksperci zbadają 11 obszarów, które mają wpływ na bezpieczeństwo informacji. Są nimi:

- polityka bezpieczeństwa
- organizacja bezpieczeństwa informacji
- zarządzanie aktywami
- bezpieczeństwo zasobów ludzkich
- bezpieczeństwo fizyczne i środowiskowe
- zarządzanie systemami i sieciami
- kontrola dostępu
- zarządzanie ciągłością działania
- pozyskiwanie, rozwój i utrzymanie systemów informatycznych
- zarządzanie incydentami związanymi z bezpieczeństwem informacji



Servus Comp Sp. z o.o. Sp. K.
30-019 Kraków ul. Mazowiecka 25/502
tel. 12 631-91-22 biuro@servus-comp.pl
https://firmapremium.zadbajobezpieczenstwo.pl

- zgodność z wymaganiami prawnymi i własnymi standardami

W czasie audytu bardzo wnikliwie weryfikowane jest bezpieczeństwo proceduralne i informatyczne, przeprowadzane są również testy oprogramowania systemowego oraz infrastruktury informatycznej. Do testów penetracyjnych używamy profesjonalnego oprogramowania, które na bieżąco jest aktualizowane o najnowsze konfiguracje sprzętowe, dzięki czemu mamy jasny obraz stanu technicznego infrastruktury.

Po przeprowadzeniu audytu sporządzimy dla Państwa poufny RAPORT identyfikujący zagrożenia
w dotychczas funkcjonującym systemie bezpieczeństwa. Raport będzie zawierał również nasze rekomendacje w zakresie rozwiązań mających zapewnić bezpieczeństwo IT oraz zalecenia
do procedur i dokumentacji.

**Otrzymują Państwo dokładny opis problemu i sugerowane rozwiązanie, jakie należy przedsięwziąć, aby zniwelować występujący problem.**

Nasz zespół to wysokiej klasy specjaliści z poszczególnych obszarów technologii IT, posiadający wiedzę nt. systemów bezpieczeństwa popartą 25-letnim doświadczeniem w branży IT.
W skład zespołu wchodzą doświadczeni audytorzy posiadający m.in. Certyfikat Audytora Wiodącego Systemu Zarządzania Bezpieczeństwem Informacji wg ISO/IEC 27001.

## Szczegółowy zakres usługi Audyt IT

- Analiza procesów zarządzania IT i bezpieczeństwem
- Przegląd dokumentacji
- Weryfikacja ochrony danych osobowych zgodnie z nową ustawą RODO
- Zbadanie zgodności konfiguracji systemów z założeniami polityki bezpieczeństwa
- Przegląd zabezpieczeń systemu informatycznego funkcjonującego w organizacji
- Przeprowadzenie testów oprogramowania systemowego
- Przeprowadzenie testów penetracyjnych infrastruktury informatycznej
- Identyfikacja słabych punktów infrastruktury IT (w tym w systemach i urządzeniach)



servus comp
Servus Comp Sp. z o.o. Sp. K.
30-019 Kraków ul. Mazowiecka 25/502
tel. 12 631-91-22 biuro@servus-comp.pl
https://firmapremium.zadbajobezpieczenstwo.pl

- Analiza potrzeb w zakresie zabezpieczenia systemu
- Dostarczenie informacji odnośnie przestrzegania norm i procedur bezpieczeństwa
- Analiza bezpieczeństwa fizycznego i środowiskowego
- Weryfikacja założeń dotyczących kontroli dostępu
- Szkolenie i transfer wiedzy do pracowników firmy
- Konsultacje poaudytowe

W ramach audytu proceduralnego audytorzy dokonują przeglądu i oceny funkcjonowania dokumentacji w następującym zakresie:

1. REGULACJE WEWNĘTRZNE

- Instrukcja Bezpieczeństwa Systemów Informatycznych
- Polityka bezpieczeństwa
- Instrukcja sporządzania informacji zarządczej
- Strategia działania firmy
- Strategia technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego
- Regulamin organizacyjny/ Schemat organizacyjny
- Instrukcja - Zasady zarządzania zmianami
- Instrukcja zarządzania ryzykiem operacyjnym
- Instrukcja - Plany awaryjne zachowania ciągłości działania w sytuacjach kryzysowych (BCP - Business Continuity)
- Instrukcja zarządzania kadrami
- Regulamin kontroli wewnętrznej i audytu
- Plan audytu wewnętrznego
- Instrukcja zarządzania ryzykiem powierzania czynności podmiotom zewnętrznym

Oraz:
Umowy z firmami zewnętrznymi w zakresie bezpieczeństwa systemów informatycznych
Polisy ubezpieczeniowe



servus comp
Servus Comp Sp. z o.o. Sp. K.
30-019 Kraków ul. Mazowiecka 25/502
tel. 12 631-91-22 biuro@servus-comp.pl
https://firmapremium.zadbajobezpieczenstwo.pl

## 2. WERYFIKACJA DOKUMENTACJI W POSZCZEGÓLNYCH OBSZARACH ZARZĄDZANIA

### Organizacja obszarów bezpieczeństwa informacji i środowiska teleinformatycznego:

Identyfikacja zagadnień i planowanie w zakresie obszarów IT
Podział zadań w zakresie bezpieczeństwa Informacji
Lista osób stanowiących kadrę rezerwową; System doskonalenia kwalifikacji/Rejestr szkoleń
Akta osobowe pracowników: Potwierdzenie kwalifikacji/odbycia szkoleń, Oświadczenia
Zakres dostępu do informacji; Separacja obowiązków pracowników

### Rozwój środowiska teleinformatycznego:

Wymagania w zakresie rozwoju systemów informatycznych
Zasady doboru komponentów infrastruktury
Standardy konfiguracyjne
Schemat dokonywania zmiany w systemach informatycznych

### Zarządzanie infrastrukturą:

Wykaz systemów informatycznych/komponentów infrastruktury
Określenie krytycznych zasobów i dostawców IT
Dziennik administratora systemu/Rejestr uprawnień/Rejestr kont serwisowych i administracyjnych
Rejestr wejść do pomieszczeń szczególnie chronionych
Dziennik sporządzania kopii/ Harmonogram testów
Procedura ponownego rozpoczęcia działalności firmy w przypadku awarii systemu informatycznego
Wykaz planów ciągłości działania i planów awaryjnych
Protokoły z testów warunków skrajnych i testów ciągłości działania
Lista kontaktowa osób i firm, które należy zawiadomić w przypadku wystąpienia sytuacji kryzysowych
Rejestr incydentów związanych z bezpieczeństwem informacji

Nasz zespół to wysokiej klasy specjaliści z poszczególnych obszarów technologii IT, posiadający wiedzę nt. systemów bezpieczeństwa popartą 25-letnim doświadczeniem



servus comp
Servus Comp Sp. z o.o. Sp. K.
30-019 Kraków ul. Mazowiecka 25/502
tel. 12 631-91-22 biuro@servus-comp.pl
https://firmapremium.zadbajobezpieczenstwo.pl

w branży IT. W ramach audytu dokonamy pełnej weryfikacji wszystkich obszarów bezpieczeństwa informacji środowiska teleinformatycznego w Państwa organizacji.

| UWAGA |
| --- |
| Państwowe organy nadzorcze zalecają w odniesienie do instytucji Państwa wykonanie audytów bezpieczeństwa informacji w zależności od wytycznych w danym sektorze w określonych ramach czasowych, a w przypadku firm biznesowych częstotliwość wykonywania audytów zależy od świadomości i wiedzy kierownictwa na ten temat . |

W celu uzyskania pełnej informacji w omawianych zakresach zapraszamy do kontaktu:

602 220 749 andrzej.popiolek@servus-comp.pl
781 555 025 anna.strek@servus-comp.pl
12 631 91 22 biuro@servus-comp.pl

Servus Comp Sp. z o.o. Sp.k.
ul. Mazowiecka 25/502, 30-019 Kraków
Sąd Rejonowy dla Krakowa – Śródmieście,
XI Wydział Gospodarczy Krajowego Rejestru Sądowego
NIP: 6772394344 | Regon: 362815411 | KRS: 0000582481

https://zadbajobezpieczenstwo.pl
https://firmapremium.zadbajobezpieczenstwo.pl
https://premiumbank.zadbajobezpieczenstwo.pl