[logotyp organizacji]

[nazwa organizacji]

PROCEDURA AUDYTU WEWNĘTRZNEGO

Kod dokumentu:	
Wersja:	
Data wersji:	
Utworzony przez:	
Zatwierdzony przez:	
Poziom poufności:	

Comment [DK1]: Aby dowiedzieć się, jak wypełniać ten dokument, zapoznaj się z wideo-szkoleniem: How to Write ISO 27001/ISO 22301 Internal Audit Procedure and Audit Program
- Jeśli zakupiłeś Pakiet, znajdziesz je w ISO 27001 & ISO 22301 Customer Portal: https://epps.customerhub.net/
- Jeśli nie zakupiłeś Pakietu, możesz zapoznać się ze skrótem szkolenia tutaj: http://advisera.com/27001academy/tutorial/documentation-tutorial-how-to-write-iso-27001iso-22301-internal-audit-procedure-and-audit-program/

Comment [DK2]: Aby dowiedzieć się więcej, przeczytaj artykuł: Dilemmas with ISO 27001 internal auditors http://advisera.com/27001academy/blog/2010/03/22/dilemmas-with-iso-27001-bs-25999-2-internal-auditors/

Comment [DK3]: Wszystkie pola oznaczone w tym dokumencie nawiasami kwadratowymi [ ] muszą być wypełnione.

Comment [DK4]: System kodowania (numeracji) dokumentów powinien być zgodny z systemem kodowania (numeracji) dokumentów stosowanym w organizacji; jeśli organizacja nie stosuje takiego systemu, ta linia może być usunięta.

©2015 Ten szablon może być używany przez klientów EPPS Services Ltd. www.advisera.com zgodnie z Umową Licencyjną.

Historia zmian

Data	Wersja	Utworzona przez	Opis zmiany
RRRR-MM-DD	0.1	Dejan Kosutic	Podstawowy szablon dokumentu

Spis treści

1. CEL, ZAKRES I UŻYTKOWNICY 3

2. DOKUMENTY REFERENCYJNE 3

3. AUDYT WEWNĘTRZNY 3

3.1. CEL AUDYTU WEWNĘTRZNEGO 3
3.2. PLANOWANIE AUDYTU WEWNĘTRZNEGO 3
3.3. WYZNACZANIE AUDYTORÓW WEWNĘTRZNYCH 4
3.4. PRZEPROWADZANIE AUDYTÓW WEWNĘTRZNYCH 4

4. ZARZĄDZANIE REJESTRAMI UTRZYMYWANYMI NA PODSTAWIE NINIEJSZEGO DOKUMENTU 5

5. WAŻNOŚĆ ORAZ ZARZĄDZANIE NINIEJSZYM DOKUMENTEM 5

6. ZAŁĄCZNIKI 6

©2015 Ten szablon może być używany przez klientów EPPS Services Ltd. www.advisera.com zgodnie z Umową Licencyjną.

1. Cel, zakres i użytkownicy

Celem niniejszej procedury jest opisanie wszystkich czynności związanych z audytem – opracowania planu audytu, wyboru audytora, przeprowadzania audytów oraz opracowania raportów z audytów.

Niniejszą procedurę stosuję do wszystkich czynności wykonywanych w zakresie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) [Systemu Zarządzania Ciągłością Działania (BCMS)].

Użytkownikami niniejszego dokumentu są [członkowie ścisłego kierownictwa] [nazwa organizacji] oraz audytorzy wewnętrzni.

Comment [DK5]: Wstawić zamiast SZBI, jeśli niniejsza procedura odnosi się wyłącznie do zarządzania ciągłością działania.

Comment [DK6]: Ciało kierownicze znajdujące się w zakresie SZBI/BCMS.

2. Dokumenty referencyjne

- Standard ISO/IEC 27001, rozdział 9.2
- Standard ISO 22301, rozdział 9.2
- Rozdział BS 25999-2, rozdział 5.1
- Polityka Systemu Zarządzania Bezpieczeństwem Informacji
- Polityka Zarządzania Ciągłością Działania
- Procedura działań korygujących i zapobiegawczych

Comment [DK7]: Usunąć, jeśli niniejsza procedura dotyczy wyłącznie zarządzania ciągłością działania.

Comment [DK8]: Usunąć, jeśli niniejsza procedura dotyczy wyłącznie zarządzania ciągłością działania.

3. Audyt wewnętrzny

3.1. Cel audytu wewnętrznego

Celem audytu wewnętrznego jest określenie, czy procedury, zabezpieczenia, procesy, uzgodnienia i inne działania w zakresie SZBI [BCMS] są zgodne z ISO 27001 oraz ISO 22301/BS 25999-2, odnośnymi [illegible] cele.

Comment [DK9]: Usunąć, jeśli niniejsza procedura dotyczy wyłącznie zarządzania ciągłością działania.

Comment [DK10]: [illegible]

3.2. Planowanie audytu wewnętrznego

[stanowisko] zatwierdzi roczny plan audytu wewnętrznego określony w Załączniku 1.

W ciągu jednego roku należy przeprowadzić jeden lub więcej audytów wewnętrznych, powinny [illegible] przeglądem dokonywanym przez kierownictwo.

Roczny program audytu wewnętrznego musi zawierać następujące informacje dotyczące każdego audytu wewnętrznego:

- okres audytu (dokładne daty lub miesiąc, w którym planowany jest audyt)
- [illegible]
- [illegible] korporacyjne i/lub zobowiązania umowne)

©2015 Ten szablon może być używany przez klientów EPPS Services Ltd. www.advisera.com zgodnie z Umową Licencyjną.

- metody audytowania (przegląd dokumentacji, wywiady z pracownikami, przegląd rejestrów, [illegible])
- [illegible] jest kierownikiem zespołu audytującego)

Przeprowadzone audyty muszą być odnotowane w Rocznym planie audytu wewnętrznego.

3.3. Wyznaczanie audytorów wewnętrznych

[stanowisko] wyznaczy audytorów wewnętrznych.

[illegible] osób na funkcję audytora wewnętrznego są następujące:

- znajomość ISO/IEC 27001 oraz ISO 22301/BS 25999-2
- [illegible]
- [illegible] tych technologii na bezpieczeństwo oraz ciągłość działania

Audytorzy wewnętrzni muszą być wybierani w sposób zapewniający ich obiektywność i neutralność, [illegible] wyników swojej własnej pracy.

Zaleca się, aby audytorzy wewnętrzni ukończyli szkolenie dla audytorów wewnętrznych normy ISO/IEC 27001.

Comment [DK11]: Usunąć, jeśli niniejsza procedura dotyczy wyłącznie zarządzania ciągłością działania.

Comment [DK12]: Usunąć, jeśli ciągłość działania nie jest wdrażana.

Comment [DK13]: Lub ISO 22301/BS 25999-2

3.4. Przeprowadzanie audytów wewnętrznych

Osoby odpowiedzialne za audyty wewnętrzne wskazane są w Rocznym planie audytu wewnętrznego. [illegible]

Podczas audytu wewnętrznego należy wziąć pod uwagę:

- kryteria określone w Rocznym planie audytu wewnętrznego
- [illegible]
- [illegible]
- Listę kontrolną audytu wewnętrznego – patrz Załącznik 3

Po wykonaniu audytu wewnętrznego należy opracować i zachować następujące dokumenty:

- Raport z audytu wewnętrznego – musi on być przesłany do [stanowisko]
- [illegible]

©2015 Ten szablon może być używany przez klientów EPPS Services Ltd. www.advisera.com zgodnie z Umową Licencyjną.

4. Zarządzanie rejestrami utrzymywanymi na podstawie niniejszego dokumentu

Nazwa rejestru	Miejsce przechowywania	Osoba odpowiedzialna za przechowywanie	Zabezpieczenia rejestru	Okres przechowywania
Roczny plan audytu wewnętrznego (w postaci elektronicznej)	Komputer [stanowisko]	[stanowisko]	Tylko [stanowisko] oraz audytor wewnętrzny mają prawo dokonywania wpisów i zmian w Rocznym planie audytu wewnętrznego.	Plany są przechowywane przez 3 lata
Raport z audytu wewnętrznego (w postaci elektronicznej)	Komputery audytora wewnętrznego oraz [stanowisko]	Audytor wewnętrzny	Raporty są przechowywane w postaci tylko do odczytu	Raporty są przechowywane przez 3 lata
Lista kontrolna audytu wewnętrznego (formularz do wypełniania podczas audytu wewnętrznego)	Komputer audytora wewnętrznego	Audytor wewnętrzny	Lista kontrolna przechowywana jest w postaci tylko do odczytu	Lista kontrolna przechowywana jest przez 3 lata

Comment [DK14]: Zwykle osoba, która zatwierdzała Roczny plan.

Comment [DK15]: Zwykle w postaci PDF

Comment [DK16]: Zwykle w postaci PDF

Tylko [stanowisko] może przydzielić innym pracownikom dostęp do do Rocznego planu audytu wewnętrznego, Raportu z audytu wewnętrznego oraz Listy kontrolnej audytu wewnętrznego.

5. Ważność oraz zarządzanie niniejszym dokumentem

Stwierdza się ważność niniejszego dokumentu na dzień [data].

[redacted]
w razie konieczności aktualizację niniejszego dokumentu, co najmniej raz do roku.

Comment [DK17]: Podany okres jest rekomendacją, należy go dostosować do wymagań organizacji.

W ocenie efektywności i właściwości niniejszego dokumentu należy wziąć pod uwagę następujące kryteria:

- [redacted]
- liczba działań korygujących wynikłych z audytu certyfikacyjnego wykonanego po audycie wewnętrznym

©2015 Ten szablon może być używany przez klientów EPPS Services Ltd. www.advisera.com zgodnie z Umową Licencyjną.

- [illegible] Rocznym planem audytu wewnętrznego Program

6. Załączniki

- Załącznik 1 – Roczny program audytu wewnętrznego
- Załącznik 2 – Raport z audytu wewnętrznego
- Załącznik 3 – Lista kontrolna audytu wewnętrznego

[stanowisko]
[imię i nazwisko]

_____
[podpis]

Comment [DK18]: Niezbędne tylko, jeśli Procedura zarządzania dokumentami I rejestrami określa, że dokumenty papierowe muszą być podpisywane.

©2015 Ten szablon może być używany przez klientów EPPS Services Ltd. www.advisera.com zgodnie z Umową Licencyjną.