

Audyt SZBI

(System Zarządzania Bezpieczeństwa Informacji)

KONTROLA	AUDYT
Wykrywa błędy formalne – głównie przepisy zewnętrzne	Wykrywa niezgodności dotyczących głównie norm wewnętrznych
Wymierza kary	Rekomenduje lepsze rozwiązania
Pełni funkcje nadzorcze / kontrolne	Pełni funkcje doradcze / usprawniające
CEL: Eliminacja błędów	CEL: Zapobieganie niezgodnościom
Ocena przeszłości	Refleksja dotycząca przyszłości
Nie uwzględnia doświadczeń innych. Każda kontrola jest oceniana indywidualnie	Odwołuje się do „najlepszych praktyk” / doświadczeń innych jednostek / firm / projektów
Kontroler posiada z mocy prawa uprawnienia operacyjne / decyzyjne	Audytora nie ma uprawnień decyzyjnych – przedstawia rekomendacje
OCENA	OCENA + REKOMENDACJE

Zadanie:

1. Na podstawie dostarczonego raportu przeprowadź audyt SZBI w firmie XYZ.
2. CELEM audytu jest ocena i poprawa (doskonalenie) poziomu SZBI (Tabela 2).
3. Przedstaw 3 REKOMENDACJE (Tabela 3) udoskonalenia SZBI w firmie XYZ w oparciu o a) zdefiniowane **priorytety** oraz b) uzyskane **oceny** (Tabela 1).

RAPORT – opis SZBI

Firma XYZ prowadzi działalność wydawniczą na terenie Polski. Ze względu na ograniczony budżet (firma działa w sektorze MŚP) udało się jedynie zrealizować niektóre postulaty w zakresie ZBI. W wyniku przeprowadzonej wizji lokalnej oraz wywiadu z kierownictwem oraz z pracownikami zebrano podstawowe informacje w zakresie funkcjonowania SZBI w badanej firmie. Obejmuje ona następujące zapisy:

W firmie istnieje niepełna dokumentacja dotycząca systemu zabezpieczenia jednostki organizacyjnej i systemu informatycznego bez wskazania osób odpowiedzialnych za realizację wytycznych w niej zdefiniowanych. Została jednakże opracowana analiza zagrożeń i ryzyk, bez wypracowania odpowiednich procedur przeciwdziałania czy też minimalizacji następstw, skutków ryzyka. Istnieją adekwatne zabezpieczenia fizyczne które obejmują serwerownie. Powstał system zarządzania uprawnieniami obejmujący wszystkie programy, systemy informatyczne wykorzystywane w firmie, zarówno w technologii stacjonarnej jak i „on-line”. Ze względów ekonomicznych, są wykorzystywane tylko darmowe, powszechnie wykorzystywane zabezpieczania danych w systemach informatycznych. Istnieje zewnętrzny nadzór administratora nad funkcjonowaniem sieci lokalnej polegający na cyklicznej (raz w miesiącu) weryfikacji oceny stanu bezpieczeństwa. Nie są w zasadzie wypracowane procedury użytkowanie notebooków służbowych jak też prywatnych. Zostały raz przeprowadzone szkolenia pracowników w zakresie SZBI. Za archiwizację danych odpowiadają kierownicy poszczególnych działów jak też sami pracownicy. Dwa lata temu został przeprowadzany audyt bezpieczeństwa przez podmiot zewnętrzny. Jednak zarząd firmy nie dostrzega korzyści wynikających z pozyskania odpowiednich certyfikatów bezpieczeństwa.

Tabela 1. LISTA PYTAŃ dotycząca audytu SZBI w firmie XYZ

Lp.	Pytania / Wytyczne / Normy	Priorytet [1-10]	Ocena nominalna [0;1;3]	Ocena ważona	Wzorzec [3]	Różnica
1	Istnieje dokumentacja dotycząca systemu zabezpieczenia jednostki organizacyjnej i systemu informatycznego ze wskazaniem osób odpowiedzialnych					
2	Została opracowana analiza ryzyka oraz zostały wdrożone procedury zarządzania ryzykiem					
3	Istnieją zabezpieczenia fizyczne obejmujące budynki i serwerownie					
4	Powstał kompleksowy system zarządzania uprawnieniami					
5	Zakupiono profesjonalne zabezpieczenia danych w systemach informatycznych					
6	Istnieje stały nadzór administratora nad funkcjonowaniem sieci lokalnej					
7	Są wypracowane procedury użytkowanie notebooków służbowych					
8	Zostały przeprowadzone szkolenia pracowników w zakresie SZBI oraz sprawdzono wymaganą wiedzę poprzez adekwatne testy / egzamin					
9	Został wdrożony system archiwizacji danych					
10	Są cyklicznie przeprowadzane audyty bezpieczeństwa przez podmioty zewnętrzne					
	RAZEM:					

Uwaga: ocena dotycząca przeprowadzonego audytu zawiera następującą skalę:

Pełna zgodność = 3 pkt. (utrzymać działania na obecnym poziomie)

Częściowa zgodność = 1 pkt. (wymagane są działa usprawniające)

Brak zgodności = 0 pkt. (konieczność natychmiastowej eliminacji niezgodności)

Tabela 2. OCENA nominalna SZBI [0-30 punktów]

Wartości [pkt]	Ocena nominalna	Wartość procentowa
0 - 10	stan wysokiego zagrożenia	do 36%
11-15	stan średniego zagrożenia	37% - 52%
16-20	stan zagrożenia	53% - 69%
21-29	stan umiarkowanego zagrożenia	70% - 99%
30	brak uzasadnionego zagrożenia	100 %

Tabela 3. WNIOSKI i REKOMENDACJE udoskonalenia SZBI w firmie XYZ

WNIOSKI (niezgodności)	REKOMENDACJE (co należy wykonać)
#10. Opis wymagania (0 pkt.). Niezgodność: ?	1. 2. 3.
	1. 2. 3.
	1. 2. 3.

Tabela 4. Ocena nominalna SZBI w firmie XYZ przed i po rekomendowanych zmianach (patrz tabela nr 2)

AS-IS (przed)	TO-BE (po)
? % zgodności	? % zgodności
<i>opis</i>	<i>opis</i>
Stan ...	