	PYTANIE	ODP1	ODP2	ODP3	ODP4	ODP5	ODP6
1	**Zarządzanie bezpieczeństwem informacji wymaga jako minimum**	Udziału akcjonariuszy	Udziału klientów	Udziału stron trzecich	Udziału pracowników	Udziału dostawców	Udziału organów państwa
2	**Wymagania dotyczące bezpieczeństwa powinny być określone w oparciu o:**	Analizy związków przyczynowo skutkowych w systemach informatycznych	Nowoczesną organizację badań bezpieczeństwa pracy	Graficzną prezentację danych dotyczących bezpieczeństwa	Szacowanie ryzyka	Zbiór wymagań prawnych, statutowych, regulacyjnych i kontraktowych	Zbiór zasad celów i wymagań opracowane przez organizację w celu wspomagania swojej działalności
3	**W definicji Zdarzenia znajdują się następujące pojęcia**	usługa	system	ludzie	błąd zabezpieczeń	przełamanie polityki bezpieczeństwa informacji	znana sytuacja
4	**Koło Deminga składa się z następujących czynności**	Sprawdzić	Działać	Planować	Policzyć	Wykonać	Uzgodnić
5	**System zarządzania bezpieczeństwem informacji odnosi się do:**	ustanowienia	doskonalenia bezpieczeństwa informacji	wdrażania bezpieczeństwa informacji	monitorowania bezpieczeństwa informacji	utrzymywania bezpieczeństwa informacji	eksploatacji bezpieczeństwa informacji
6	**Zabezpieczenie to**	praktyka	środki zarządzania ryzykiem	zalecenia	procedury	teoria	struktury organizacyjne
7	**Źródła zagrożeń to**	niewłaściwa administracja systemem informatycznym	zaniedbania i błędy użytkowników	niezadowolenie pracowników	ingerencje intruzów	możliwość podsłuchu	retransmisja informacji
8	**Znamy następujące rodzaje audytów w bezpieczeństwie informacji**	Audyt systemu zarządzania bezpieczeństwem informacji	Audyt bezpieczeństwa informacji	Audyt ochrony danych bezosobowych	Analiza podatności	Testy penetracyjne	Audyt systemów finansowo - księgowych
9	**Rodzaje zagrożeń to**	uprawniona modyfikacja informacji	powielenie komunikatu	kradzież istotnych informacji	sabotaż zasobów	niezaprzeczenie wykonania operacji	staranność użytkowników
10	**Obraźliwa i nielegalna treść to**	Nielegalne transakcje	promowanie terroryzmu	paserstwo	promowanie firmy	pedofilia	promowanie antyglobalizmu
11	**Przykładowymi zagrożeniami jest**	pożar	wypadek przemysłowy	słońce	kurz	legalne użycie oprogramowania	obciążenie ruchem
12	**Zagrożenia przypadkowe to**	infiltracja transmisji	uszkodzenie linii	niewłaściwe trasowanie wiadomości	analiza ruchu	niedobór personelu	właściwe wykorzystanie zasobów
13	**Najgrożniejsze wycieki informacji w 2008i9r to**	Odsprzedaż daych osobowych przez firmę Gratis Internet COmpany	Kradzież danych osobowych administracji prezydenta Busha	zgubienie nootebooka z firmy Dell z danymi osobowymi klientów	kradzież laptopa pracownika Nationwide building Society	z biura microsoft skradziono przenośny komputer zawierający dane pracowników	Ujawnienie przez AOL zapytań i nazwisk użytkowników
14	**Ustanowienie SZBI obejmuje**	zdefiniowanie zakresu Organizacji	zdefiniowanie granic SZBI	dokładny opis i uzasadnienie dla każdego wyłączenia z zakresu	politykę SZBI	deklarację stosowania	sformułowania pranu postępowania z ryzykiem

15	**Monitorowanie i przegląd SZBI obejmuje**	Wykonywanie pomiaru skuteczności SZBI	Wykonywanie pomiaru skuteczności zabezpieczeń	Wykonywanie przeglądów ryzyka	Przeprowadzanie wewnętrznych audytów	Uaktualnianie planów bezpieczeństwa	rejestrowanie działań mających wpływa na skuteczność i wydajność realizacji SZBI
16	**Utrzymywanie i doskonalenia SZBI obejmuje**	wdrażanie w SZBI zidentyfikowanych udoskonaleń	podejmowanie odpowiednich działań korygujących	informowanie wszystkich zainteresowanych stron o działaniach i udoskonaleniach	Udoskonalanie metodyki zarządzania ryzykim	podejmowanie odpowiednich działań zapobiegawczych	zapewnienie że udoskonalenie nie spełniają zamierzonych celów
17	**Dokumentacja powinna obejmować**	zapisy decyzji organów nadrzędnych	cele	zakres SZBI	zabezpieczenia wspomagające SZBI	raport z procesu szacowania ryzyka	deklarację zgodności
18	**Zapisy powinny dotyczyć**	udokumentowanej procedury	realizacji procesów	polityki bezpieczeństwa informacji	deklaracji zgodności	wszystkich incydentów	celów stosowania zabezpieczeń
19	**Odpowiedzialność kierownictwa obejmuje**	ustanowienie polityki wdrożenia SZBI	zapewnienia że cele i plany SZBI zostały ustanowione	Dążenie do stworzenia zaufania	zapewnienie wystarczających zasobów	podejmowanie decyzji o kryteriach akceptowania ryzyka	zapewnienie przeprowadzenia wewnętrznych audytów SZBI
20	**Szkolenie, uświadamianie i kompetencje obejmują**	certyfikację SZBI	wdrożenie procedury reakcji na incydenty	zapewnienie braku zaangażowania pracowników	Orientacja na wzrost kosztów zabezpieczeń	Podejmowanie decyzji na podstawie analizy efektów SZBI	Korzystne dla dostawców stosunki z organizacją
21	**Dane wejściowe do przeglądu to**	zalecenia dotyczące doskonalenia	działania poprzeglądowe	status działań zapobiegawczych	podatności niepoprawnie przypisane	wyniki pomiaru skuteczności	techniki nadające się do doskonalenia SZBI
22	**Dane wyjściowe z przeglądu to**	modyfikacja procedur bezpieczeństwa informacji	zapewnienie zgodności SZBI z potrzebami klenta	wymagane zasoby	Ustanawianie nowoczesnych metod ścisłej kontroli pracy	uaktualnienia planu szacowania ryzyka	udoskonalenie metod pomiaru skuteczności zabezpieczeń
23	**Procedury wymagane przez ISO/IEC 27001:2005**	Nadzór nad dokumentacją	Nadzór nad zapisami	Postępowanie z systemem niezgodnym	Działania korygujące	Działania doskonalące	Audit wewnętrzny
24	**Doskonalenie SZBI powinno być realizowane poprzez**	stosowanie polityki bezpieczeństwa informacji	działania zapobiegawcze	Działania dyscyplinujące	określanie celów bezpieczeństwa	wyniki audytów	analizę monitorowanych zdarzeń
25	**Rola kierownictwa w ISO/IEC 27001:2005**	Jest pomijalnie mała	nigdzie nie jest określona w normie bo jest nieistotna	ma znaczenie ale najważniejsze jest zapewnienie odpowiedniego sprzętu	Jest ważna ponieważ kierownictwo przydziela zasoby na zakup nowych systemów informatycznych	Jest ograniczona do testów penetracyjnych	Jest ważna tylko w przypadku kontaktów z organamii władzy
26	**Działania zapobiegawcze**	to inna nazwa działań korygujących	mają na celu wyeliminowanie zagrożeń	mają za zadanie ochronę przed potencjalnymi niezgodnościami	powinny być realizowane zgodnie z udokumentowaną procedurą	powinny być priorytetyzowane w oparciu o wyniki szacowania ryzyka	mają na celu wyeliminowanie przyczyn niezgodności
27	**Polityka SZBI**	zawiera ramy ustalania celów	bierze pod uwagę wymagania biznesowe	ustanawia kontekst strategiczny zarządzania ryzykiem	wyznacza ogólny kierunek dotyczący bezpieczenstwa informacji	określa kryteria według których ma być oceniane ryzyko	została zaakcceptowana przez kierownictwo
28	**Norma ISO/IEC 27001 wymaga następujących działań w odniesieniu do ryzyka**	wskazać metodykę szacowania ryzyka	wybrana metodyka powinna zapewnić nieporównywalne i niepowtarzalne rezultaty	określić akceptowane poziomy ryzyka	określić tylko aktywa informacyjne	określić skutki utraty integralności	określić szkody i straty dla biznesu, które mogą wynikać z naruszenia bezpieczeństwa

29	**Doskonalenie**	Wchodzi w skład działań korygujących	NIe powinno być realizowane za pomocą cyklu Deminga	Wchodzi w skład działań zapobiegawczych	Jest realizowane w ramach testów penetracyjnych	Stanowi element planu zapewnienia bezpieczeństwa	Powinno być stosowane tylko w odniesieniu do zapisów
30	**Warianty postępowania z ryzykiem obejmuję**	poznanie ryzyk w sposób nieświadomy	zaakceptowanie ryzyk	unikanie ryzyk	ignorowanie ryzyk	przeniesienie ryzyk do innych uczestników	zastosowanie zabezpieczeń
31	**Przeglądy ryzyka akceptowalnego powinny brać pod uwagę**	zmiany organizacji	zmiany skuteczności stosowanych zabezpieczeń	zmiany zidentyfikowanych zagrożeń	zdarzenia zewnętrzne	zmiany celów i procesów biznesowych	zmiany technologii
32	**Przykładowe aktywa to**	zbiory danych	procedury wsparcia	oprogramowanie użytkowe	laptopy	automatyczne sekretarki	CD
33	**Usługi wchodzące w skład aktywów to**	usługi obliczeniowe	zasilanie	klimatyzacja	ogrzewanie	transport	usługi telekomunikacyjne
34	**Przykładowe podatności to**	stabilna sieć elektryczna	lokalizacja na terenie zagrożonym powodzią	podatność na zmiany temperatury	wadliwa instalacja nośników	brak sprawnej kontroli zmian w konfiguracji	linie komutowane
35	**Przykładowe podatności dotyczące oprogramowania to**	Chronione tablice haseł	Brak kontroli pobierania i używania oprogramowania	brak dokumentacji	brak codziennej kontroli zmian	brak śladów dla audytu	skomplikowany interfejs dla użytkowników
36	**W przykładowej metodzie analizy ryzyka stosowane są następujące termin**	skutek katastrofalny	ryzyko niskie	ryzyko przeciętne	skutek znaczący	ryzyko pomijalne	skutek istotny
37	**Norma ISO/IEC 27002 (poprzednio o nazwie ISO/IEC 17799) zawiera w rozdziale organizacja wewnętrzna następujące punkty**	zaangażowanie kierownictwa w bezpieczeństwo informacji	kontakty z organami władzy	umowy o zachowaniu tajności	proces autoryzacji pracowników	przypisanie odpowiedzialności w zakresie bezpieczeństwa	forum bezpieczeństwa informacji
38	**W przypadku kontaktów ze stronami zewnętrznymi podstawą jest**	bezpieczeństwo w umowach ze stroną piątą	bezpieczeństwo w kontaktach z dostawcami	określenie ryzyk związanych z pracownikami	bezpieczeństwo w kontaktach z akcjonariuszami	bezpieczeństwo w kontaktach z organami władzy	bezpieczeństwo w kontaktach z forum bezpieczeństwa inforamcji
39	**Bezpieczeństwo zasobów ludzkich obejmuje**	ochronę przed wypadkami	zwrot pasywów	postępowanie dyscyplinarne	zasady i warunki zatrudnienia	odebranie praw dostępu	odpowiedzialność związaną z zakończeniem postępowania sprawdzającego
40	**Audyt systemu zarządzania bezpieczeństwem informacji to**	Kontrola pracy wykonywanej przez pracowników	systematyczne i niezależne badanie zdolności systemu informatycznego	systematyczne i niezależne badanie, mające określić czy działania odpowiadają uzgodnieniom z dostawcą	systematyczne i niezależne badanie, mające określić czy zabezpieczenia są skutecznie realizowane	systematyczne i niezależne badanie, mające określić czy działania przynoszą wymierny zysk	systematyczne i niezależne badanie, mające określić czy działania pozwalają na osiągnięcie celów SZBI
41	**Audyt Certyfikacyjny obejmuje**	przegląd dokumentacji analizy ryzyka	przegląd dokumentacji kluczowych elementów SZBI	raport z 1 etapu	zaplanowanie 2 etapu	potwierdzenie że organizacja realizuje własną politykę	przygotowanie raportu z audytu w celu podjęcia decyzji co do certyfikacji
42	**Drugi etap audytu certyfikacyjnego koncentruje się na**	związkach pomiędzy polityką, wynikami oceny zagrożenia i in.	odpowiedzialności kierownictwa za politykę bezpieczeństwa informacji	przeglądach bezpieczeństwa i zarządzania	celach wynikających z polityki	deklaracji stosowania	ocenie ryzyka związanego z bezpieczeństwem informacji

45	**Programy antywirusowe można oceniać ze względu na**	wielkość plików łatek	szybkość skanowania	obsługę techniczną	wsparcie	interakcję z innymi programami antywirusowymi	możliwość używania bez podłączenia z internetem
46	**Programy antyspamowe można instalować**	na routerach	na serwerach	wbudować w programy pocztowe	wbudowane w programy antywirusowe	stosować jako odrębne oprogramowanie	wbudowane w system operacyjny
47	**Komponenty firewall**	filtry pakietów	bramy na poziomie warstwy transportowej	bramy na poziomie aplikacji	wielopoziomowe zapory z badaniem złego stanu połączeń	przełączniki	oprogramowanie antyspamowe
48	**Celami audytu systemu zarządzania bezpieczeństwem informacji jest**	stwierdzenie zgodności SZBI z wymaganiami	wykrycie niezgodności SZBI z wymaganiami	ustalenie skuteczności wdrożonego SZBI	Umożliwienie audytorowi poprawy SZBI	spełnienie wymagań wynikających z przepisów prawa	Umożliwienie rejestracji SZBI w urzędzie państwowym
49	**Odpowiedzialność audytora dotyczy**	Spełnienia wymagań związanych z audytem	Przekazywania wymagań związanych z auditem	Zapewnienia satysfakcji kierownictwa	Zapewnienia satysfakcji zainteresowanych stron	Ochrony dokumentów dotyczących audytu	Wspieranie audytora wiodącego
50	**Zadania audytora i audytora wiodącego**	Określenie wymagań dotyczących zadań auditu	Zaplanowanie auditu	Niezwłoczne informowanie przełożonego/klienta) o krytycznych niezgodnościach	informowanie o poważnych przeszkodach napotykanych podczas audytu	jasne przedstawianie wyników audytu	postępowanie w sposób etyczny
43	**Plan audytu obejmuje**	termin dostarczenia raportu z audytu	harmonogram spotkań	określenie zespołu audytowego	Identyfikację powiązanych dokumentów	datę i miejsca wykonania auditu	umowa o zachowaniu poufności
44	**Programy antywirusowe**	Chonią przed specjalnie napisanym dla zaszkodzenia naszej firmie oprogramowaniem	Chronią przed backdoor	Chronią przed zainstalowaniem niepotrzebnych programów	NIe chronią przed robakami internetowymi	Chronią przed atakiem z internetu	Zupełnie nie chronią przed koniami trojańskimi
51	**Bezpieczeństwo informacji oznacza**	dostępność	wiarygodność	integralność	tajność	zaprzeczalność	niezawodność
52	**Bezpieczeństwo informacji można osiągnąć stosując**	procedury	sprzęt	funkcje oprogramowania	struktury organizacyjne	proces bezpieczeństwa	dobre praktyki
53	**Normy rodziny ISO 27000 to**	ISO/IEC 17799	ISO/IEC 27006	ISO/IEC 27009	ISO/IEC 15408	ISO/IEC 27002	ISO/IEC 18043
54	**Przykłady zagrożeń to:**	Włamanie do systemu	pożar	Wypadki pracowników	Skasowanie pliku	złośliwy kod	donos
55	**Kod złośliwy to:**	koń trojański	backdoor	wirus	robak internetowy	bomba logiczna	bakteria
56	**PN ISO/IEC 27001 składa się z następujących rozdziałów:**	wprowadzenia	terminologii i definicji	doskonalenia SZBI	załącznika B zasady OECD	załącznika D różnice w porównaniu do poprzedniego wydania normy	procesu zarządzania bezpieczeństwem informacji
57	**Wdrożenie i eksploatacja SZBI obejmuje**	zarządzanie zasobami SZBI	przygotowanie deklaracji stosowania	wdrożenie programów szkolenia i uświadamiania	szacowanie ryzyka	definiowanie jak mierzyć skuteczność zabezpieczeń i grup zabezpieczeń	wdrożenie zabezpieczeń tak aby osiągnąć cel stosowania zabezpieczeń
58	**Wymagane procedury w SZBI to**	nadzór nad dokumentacją	nadzór nad zapisami	audyty wewnętrzne	działania doskonalące	postępowanie z wyrobem niezgodnym	natychmiastowego wykrycia incydentów i reakcji na zdarzenia związane z bezpieczeństwem informacji

59	**Podstawowe definicje związane z zarządzaniem ryzykiem to:**	postępowanie z ryzykiem	traktowanie ryzyka	ryzyko nieuzasadnione	zagrożenia	podatności	pasywa
60	**Model zarządzania ryzykiem wg. ISO/IEC 27005 obejmuje**	minimalizowanie ryzyka	doskonalenie ryzyka	planowanie ryzyka	maksymalizowanie ryzyka	weryfikowanie ryzyka	walidowanie ryzyka