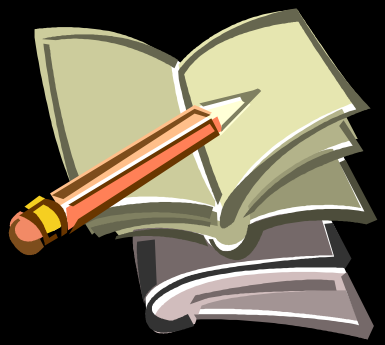
System zarządzania bezpieczeństwem informacji

PYTANIA sprawdzające

– test wyboru



dr Marian Krupa

Instrukcja:

1. Test jednokrotnego wyboru, tj. należy wskazać TYLKO na jedną odpowiedź.
2. Należy zwrócić uwagę na twierdzenia przeczące, np. „Wskaż fałszywe stwierdzenie”.
3. Należy krotko uzasadnić odpowiedzi.
4. Rozwiązany test należy opracować w formie tabeli (patrz przykład) i przesłać na adres wykładowcy w formacie pdf!

Nr	Odpowiedź	Krótkie uzasadnienie

Pytania: 1

Zagrożenie to:

A.	potencjalna możliwość naruszenia bezpieczeństwa systemu informatycznego.
B.	wady lub luki w strukturze fizycznej organizacji, procedurach, zarządzaniu, administrowaniu, sprzęcie i oprogramowaniu.
C.	Odpowiedzi A i B są prawidłowe.

Pytania: 2

Ryzyko to:

A.	iloczyn częstości (prawdopodobieństwa) zdarzenia przez miarę strat spowodowanych tym zdarzeniem (albo wartość aktywu).
B.	rezultat niepożądanego incydentu.
C.	praktyka, procedura lub mechanizm ograniczający sprawność działania systemu.

Pytania: 3

Do podstawowych funkcji zabezpieczeń należą:

A.	wykrywanie, ograniczanie, zapobieganie, odtwarzanie.
B.	uświadamianie, monitorowanie, poprawianie.
C.	Odpowiedzi A i B są prawidłowe.

Pytania: 4

Wskaż fałszywe stwierdzenie:

A.	Mechanizmy kontrolne mogą mieć charakter prewencyjny, detekcyjny i korekcyjny.
B.	Polityka bezpieczeństwa powinna być spisana w formie dokumentu, z którym należy selektywnie zapoznać wszystkich użytkowników systemu informatycznego organizacji.
C.	Polityka bezpieczeństwa instytucji i polityka bezpieczeństwa informacji to terminy tożsame, stosowane wymiennie.

Pytania: 5

Do najistotniejszych procesów wchodzących w skład zarządzania bezpieczeństwem systemów informatycznych można zaliczyć:

A.	zarządzanie ryzykiem, zarządzanie jakością.
B.	zarządzanie konfiguracją, zarządzanie zmianami, zarządzanie ryzykiem.
C.	Żadna z powyższych odpowiedzi nie jest prawidłowa.

Pytania: 6

Zarządzanie konfiguracją ma gwarantować:

A.	wprowadzanie zmian, które nie obniżą efektywności funkcjonowania systemu, skuteczności mechanizmów zabezpieczających oraz ogólnego bezpieczeństwa organizacji.
B.	wprowadzanie stosownych zmian dotyczących planowania ciągłości działania i odtwarzania po katastrofie.
C.	Odpowiedzi A i B są prawidłowe.

Pytania: 7

W obszarze zarządzania zmianami audytor powinien zweryfikować:

A.	istnienie procedur gwarantujących, że w rejestrze zasobów wskazane są wyłącznie istniejące i autoryzowane składniki konfiguracji.
B.	aktualność, spójność i kompletność rejestru konfiguracji.
C.	Odpowiedzi A i B są prawidłowe.

Pytania: 8

Efektywny program zarządzania ryzykiem powinien zapewniać osiągniecie celów biznesowych organizacji przez:

A.	skuteczniejsze zabezpieczenie systemów informatycznych, które przechowują, przetwarzają i przesyłają informacje należące do organizacji.
B.	umożliwienie kierownictwu uzasadnienia swych decyzji dotyczących wydatków na zarządzanie ryzykiem zaplanowanych w budżecie.
C.	Odpowiedzi A i B są prawidłowe.

Pytania: 9

Wskaż fałszywe stwierdzenie:

A.	ISMS dotyczy struktury organizacyjnej, polityki, zaplanowanych działań, zakresów odpowiedzialności, zasobów, procesów oraz procedur.
B.	na proces planowania i implementacji ISMS wpływają potrzeby i cele biznesowe, wymagania bezpieczeństwa, wykonywane procesy oraz wielkość i struktura jednostki.
C.	Skrót ISMS oraz SZBI nie są tożsame.

Pytania: 10

Wskaż prawdziwe stwierdzenie.

Polityka ISMS:

A.	powinna zawierać cele i zasady działania dotyczące zarządzania bezpieczeństwem informacji.
B.	nie musi być zaakceptowana przez kierownictwo.
C.	nie wskazuje kryteriów szacowania ryzyka.

Pytania: 11

Wśród wariantów traktowania ryzyka można wskazać:

A.	wdrożenie zabezpieczeń, unikanie ryzyka, zaakceptowanie ryzyka, transfer ryzyka.
B.	tylko wdrożenie zabezpieczeń, unikanie ryzyka.
C.	Żadna z powyższych odpowiedzi nie jest prawidłowa.

Pytania: 12

Wskaż fałszywe stwierdzenie:

A.	Wewnętrzne audyty ISMS powinny być prowadzone regularnie i odpowiednio zaplanowane.
B.	W programie audytu należy wskazać kryteria, zakres, częstotliwość i przyjętą metodykę audytu.
C.	Nie obowiązuje tu zasada niezależności audytora, który może badać swoja własną pracę.

Pytania: 13

Audyt to:

A.	specyficzne postępowanie o charakterze poświadczającym prowadzone przez niezależną jednostkę.
B.	weryfikacja zgodności systemu kontroli wewnętrznej z określonymi wymaganiami, standardami lub procedurami.
C.	Odpowiedzi A i B są prawidłowe.

Pytania: 14

Audyt bezpieczeństwa informacyjnego to:

A.	systematyczny, niezależny i udokumentowany proces uzyskiwania dowodu z audytu oraz jego obiektywnej oceny.
B.	systematyczny, niezależny i udokumentowany proces uzyskiwania dowodu z audytu oraz jego obiektywnej oceny w celu ciągłego doskonalenia systemu ZBI.
C.	systematyczny, niezależny i udokumentowany proces uzyskiwania dowodu z audytu oraz jego obiektywnej oceny w celu zdefiniowania poziomu niezgodności systemu ZBI.

Pytania: 15

Audyt bezpieczeństwa informacyjnego nie obejmuje:

A.	weryfikacji poziomu bezpieczeństwa systemów informatycznych.
B.	analizy ryzyka związanego z prowadzeniem projektu informatycznego.
C.	Oceny poziomu innowacyjności systemów informatycznych.

Pytania: 16

Najwcześniejszą dziedzina, w której audyt znalazł zastosowanie jest:

A.	badanie sprawozdań finansowych przedsiębiorstw.
B.	badanie systemów informatycznych.
C.	badanie systemu zarządzania jakością.

Pytania: 17

Wskaż fałszywe stwierdzenie:

A.	Celem fazy planowania modelu PDCA jest ustanowienie polityki bezpieczeństwa oraz procedur dla zarządzania ryzykiem i doskonalenia ISMS.
B.	Na etapie wykonania ma miejsce wdrożenia i eksploatacja przyjętej polityki bezpieczeństwa, zabezpieczeń i procedur..
C.	W tramach fazy wykonania należy wdrożyć dodatkowe mechanizmy kontrolne zabezpieczające przed akceptowalnym ryzykiem.

Pytania: 18

Jakie techniki testowania można wykorzystać w ramach fazy sprawdzania modelu PDCA?

A.	Rutynowe sprawdzanie, samokontrolujące się procedury, uczenie się od innych, wewnętrzne audyty ISMS.
B.	Przeglądy realizowane przez kierownictwo, analizę trendów.
C.	Odpowiedzi A i B są prawidłowe.

Pytania: 19

Celem fazy działania jest:

A.	podjęcie odpowiednich czynności naprawczych oraz zapobiegawczych na podstawie wniosków kierownictwa wyciągniętych z przeprowadzonych w fazie sprawdzania testów.
B.	wdrożenia i eksploatacja przyjętej polityki bezpieczeństwa, zabezpieczeń i procedur..
C.	identyfikacja i szacowanie rodzajów ryzyka, na jakie narażone jest organizacja.

Pytania: 20

Plan postępowania z ryzykiem:

A.	wskazuje czynności podjęte dla zredukowania nieakceptowanych poziomów ryzyka i implementacji odpowiednich zabezpieczeń.
B.	nie zawiera terminu wdrożenia zabezpieczeń.
C.	Nie uwzględnia zabezpieczeń dodatkowych.