Cyberbezpieczeństwo

Topical Requirement

Wymagania Tematyczne

Przetłumaczone przez:

The Institute of Internal Auditors

Instytut Audytorów Wewnętrznych IIA Polska

Wymagania Tematyczne w obszarze cyberbezpieczeństwa

Międzynarodowe Ramy Praktyk Zawodowych (International Professional Practices Framework®) obejmują Globalne Standardy Audytu Wewnętrznego (Global Internal Audit Standards™), Wymagania Tematyczne (Topical Requirements) oraz Globalne Wytyczne (Global Guidance). Wymagania tematyczne są obowiązkowe i muszą być stosowane w połączeniu ze Standardami, które stanowią wiarygodną podstawę dla wymaganych praktyk.[1]

Wymagania Tematyczne przedstawiają jasno określone oczekiwania wobec audytorów wewnętrznych poprzez ustanowienie minimalnego zestawu wymagań dla audytu określonych obszarów ryzyka. Profil ryzyka organizacji może wymagać od audytorów wewnętrznych uwzględnienia dodatkowych aspektów audytowanego obszaru.

Zgodność z Wymaganiami Tematycznymi prowadzi do zwiększenia spójności usług audytu wewnętrznego oraz do poprawy jakości i wiarygodności tych usług oraz wyników audytu wewnętrznego. Co więcej, Wymagania Tematyczne podnoszą rangę zawodu audytora wewnętrznego.

Audytorzy wewnętrzni muszą stosować Wymagania Tematyczne zgodnie z Globalnymi Standardami Audytu Wewnętrznego. Zgodność z Wymaganiami Tematycznymi jest obowiązkowa dla usług zapewniających i jest zalecana dla usług doradczych.

Wymagania Tematyczne mają zastosowanie, gdy zagadnienie dotyczące cyberbezpieczeństwa jest:

A. ujęte w planie audytu wewnętrznego,
B. zidentyfikowane podczas zadania audytowego,
C. przedmiotem zadania, które nie zostało uwzględnione w pierwotnym planie audytu wewnętrznego.

[1] (Uwaga do tłumaczenia polskiego) Termin „kontrola" należy rozumieć zgodnie z definicją zawartą w słowniku GSAW, jako każde działanie podjęte przez kierownictwo, radę i inne strony w celu zarządzania ryzykiem i zwiększenia prawdopodobieństwa osiągnięcia ustalonych celów. W kontekście cyberbezpieczeństwa pojęcie to obejmuje również zabezpieczenia i środki zapobiegawcze/zaradcze (ang. safeguards, countermeasures) zgodnie z terminologią ISACA.

Należy udokumentować i zachować dowody na to, że każdy wymóg z Wymagań Tematycznych został oceniony pod kątem zasadności zastosowania. Nie wszystkie pojedyncze wymogi muszą mieć zastosowanie do każdego zadania; jeśli któreś wymogi są wyłączone, należy udokumentować i zachować uzasadnienie. Zgodność z Wymaganiami Tematycznymi jest obowiązkowa i zostanie oceniona podczas oceny jakości.

Więcej informacji można znaleźć w Poradniku Wymagań Tematycznych dotyczących cyberbezpieczeństwa.

Cyberbezpieczeństwo

Narodowy Instytut Standardów i Technologii (NIST) definiuje cyberbezpieczeństwo jako "zdolność do ochrony lub obrony funkcji cyberprzestrzeni przed cyberatakami". Cyberbezpieczeństwo jest podzbiorem bezpieczeństwa informacji, które jest pojęciem szerszym i które NIST definiuje jako "ochronę informacji i systemów informatycznych przed nieautoryzowanym dostępem, wykorzystaniem, ujawnieniem, zakłóceniem, modyfikacją lub zniszczeniem, w celu zapewnienia poufności, integralności i dostępności".

Cyberbezpieczeństwo ogranicza ryzyko poprzez wzmacnianie systemu kontroli oraz zabezpieczanie zasobów informacyjnych organizacji przed nieautoryzowanym dostępem, ingerencją w integralność danych, zakłóceniem ciągłości działania lub ich zniszczeniem. Cyberataki mogą wywołać bezpośrednie i pośrednie skutki, które często są znaczące, ponieważ komputery, sieci, oprogramowanie, dane i informacje wrażliwe są krytycznymi zasobami większości organizacji.

Ewaluacja i ocena ładu organizacyjnego, zarządzania ryzykiem i kontroli w obszarze cyberbezpieczeństwa

Niniejsze Wymagania Tematyczne zapewniają spójne, wyczerpujące podejście do oceny projektu i wdrożenia procesów ładu organizacyjnego, zarządzania ryzykiem i zabezpieczeń w obszarze cyberbezpieczeństwa. Wymagania te stanowią minimalny punkt odniesienia dla oceny cyberbezpieczeństwa w organizacji.

ŁAD ORGANIZACYJNY: Ewaluacja i ocena ładu organizacyjnego cyberbezpieczeństwa

Wymagania:

Audytorzy wewnętrzni muszą ocenić następujące kwestie w odniesieniu do ładu organizacyjnego cyberbezpieczeństwa w organizacji:

A. Formalna strategia i cele w zakresie cyberbezpieczeństwa są ustanowionei okresowo aktualizowane. Bieżące informacje dotyczące osiągania celów w zakresie

cyberbezpieczeństwa są okresowo przekazywane i przeglądane przez radę, z uwzględnieniem budżetu i zasobów wspierających strategię cyberbezpieczeństwa.

B. Polityki i procedury związane z cyberbezpieczeństwem są ustanowione i okresowo aktualizowane w celu wzmocnienia środowiska kontroli.

C. Role i obowiązki, które wspierają osiąganie celów cyberbezpieczeństwa, są ustanowione, oraz istnieje proces okresowej oceny wiedzy, umiejętności i zdolności osób pełniących te role.

D. Odpowiedni interesariusze są zaangażowani w omawianie i podejmowanie działań w związku z istniejącymi podatnościami i pojawiającymi się zagrożeniami w środowisku cyberbezpieczeństwa. Do interesariuszy zaliczamy: kierownictwo wyższego szczebla, osoby odpowiedzialne za operacje, zarządzanie ryzykiem, kadry, pracowników działów prawnych, działów zapewniania zgodności, dostawców i innych.

ZARZĄDZANIE RYZYKIEM: Ewaluacja i ocena procesu zarządzania ryzykiem cyberbezpieczeństwa

Wymagania:

Audytorzy wewnętrzni muszą ocenić następujące kwestie w odniesieniu do zarządzania ryzykiem cyberbezpieczeństwa organizacji:

A. Procesy oceny ryzyka i zarządzania ryzykiem w organizacji obejmują identyfikowanie, analizowanie, łagodzenie i monitorowanie zagrożeń cyberbezpieczeństwa oraz ich wpływu na osiąganie celów strategicznych.

B. Zarządzanie ryzykiem cyberbezpieczeństwa jest prowadzone w całej organizacji i może obejmować następujące obszary: technologia informacyjna, zarządzanie ryzykiem korporacyjnym, zasoby ludzkie, prawo, zgodność, operacje, łańcuch dostaw, księgowość, finanse i inne.

C. Ustanowiono rozliczalność i odpowiedzialność w obszarze zarządzania ryzykiem cyberbezpieczeństwa. Wyznaczono osobę lub zespół do okresowego monitorowania i raportowania w zakresie sposobu zarządzania ryzykiem cyberbezpieczeństwa, w tym zasobów wymaganych do łagodzenia ryzyka i identyfikowania pojawiających się zagrożeń cyberbezpieczeństwa.

D. Ustanowiono proces szybkiej eskalacji każdego ryzyka cyberbezpieczeństwa (nowo-pojawiającego się lub wcześniej zidentyfikowanego), które osiąga niedopuszczalny poziom zgodnie z ustalonymi wytycznymi organizacji dotyczącymi zarządzania ryzykiem lub obowiązującymi wymogami prawnymi i regulacyjnymi. Należy rozważyć finansowe i niefinansowe skutki ryzyka cyberbezpieczeństwa.

E. Ustanowiono procesy oddziaływania na świadomość kierownictwa i pracowników w zakresie ryzyka związanego z cyberbezpieczeństwem oraz okresowego przeglądu przeprowadzanego przez kierownictwo, odnośnie napotkanych problemów, luk, braków i awarii lub nieprawidłowości w działaniu kontroli, wraz z terminowym raportowaniem i podejmowaniem działań naprawczych.

F. Organizacja wdrożyła proces reagowania i odtworzenia działalności w związku z incydentami cyberbezpieczeństwa. Proces ten obejmuje wykrywanie, ograniczanie strat, odtworzenie i analizę po incydencie. Procesy reagowania na incydenty oraz odtworzania działalnoiści w związku z incydentami cyberbezpieczeństwa są okresowo testowane.

KONTROLE - Ewaluacja i ocena procesów kontroli cyberbezpieczeństwa

Wymagania:

Audytorzy wewnętrzni muszą ocenić następujące kwestie w odniesieniu do procesów kontroli w obszarze cyberbezpieczeństwa:

A. Ustanowiono proces mający na celu zapewnienie funkcjonowania zarówno kontroli wewnętrznatrz organizacji, jak i kontroli dotyczących dostawców w celu ochrony poufności, integralności i dostępności systemów i danych organizacji. Okresowo przeprowadzane są oceny w celu ustalenia, czy mechanizmy kontrolne funkcjonują w sposób sprzyjający osiągnięciu celów organizacji w zakresie cyberbezpieczeństwa i szybkiemu rozwiązywaniu problemów.

B. Ustanowiono proces zarządzania talentami, który obejmuje szkolenia w celu rozwijania i utrzymywania kompetencji technicznych związanych z operacjami cyberbezpieczeństwa. Proces ten jest okresowo poddawany przeglądowi.

C. Ustanowiono proces ciągłego monitorowania i zgłaszania pojawiających się zagrożeń i podatności w obszarze cyberbezpieczeństwa oraz identyfikowania, priorytetyzacji i wykorzystywania możliwości doskonalenia operacji w zakresie cyberbezpieczeństwa.

D. Cyberbezpieczeństwo jest uwzględnione w zarządzaniu cyklem życia (wybór, użytkowanie, konserwacja i wycofanie z eksploatacji) wszystkich zasobów IT, w tym sprzętu, oprogramowania i usług dostawców.

E. Ustanowiono procesy mające na celu wzmocnienie cyberbezpieczeństwa, obejmujące konfigurację, administrację urządzeniami użytkowników końcowych, szyfrowanie, zarządzania poprawkami oprogramowania (tzw. patchowanie), zarządzanie dostępem użytkowników oraz monitorowanie dostępności i działania. Kwestie cyberbezpieczeństwa są uwzględniane przy tworzeniu oprogramowania (DevSecOps).

F. Ustanowiono kontrole związane z siecią, takie jak kontrole zabezpieczenia dostępu do sieci i segmentacja sieci; użycie i rozmieszczenie zapór sieciowych (tzw. firewall); ograniczanie połączeń z i do sieci zewnętrznych; wirtualna sieć prywatna (VPN) / stosowanie zasad zerowego zaufania w dostępach do sieci` (ang. ZTNA - zero trust network access); zabezpieczenia sieciowe urządzeń IoT (ang. Internet of Things); oraz systemy wykrywania / zapobiegania włamaniom (IDS i IPS).

G. Kontrole bezpieczeństwa komunikacji punktów końcowych są ustanawiane dla usług takich jak poczta e-mail, przeglądarki internetowe, wideokonferencje, komunikatory, media społecznościowe, chmura i protokoły współdzielenia plików.

Serdecznie dziękujemy zespołowi tłumaczy za ich ciężką pracę oraz nieoceniony wkład, który pomógł poprawić jakość tłumaczenia.

Poniżej nazwiska osób, które sprawiły, że tłumaczenie tej publikacji było możliwe:
Marcin Dublaszewski, CIA, CGAP, CRMA, LA ISO 27001
Piotr Dzwonkowski, CISA, CISM, CRISC
dr Romana Kawiak-Ciołak, CIA, CRMA, QA, MPA, CCPF, EITCA/AI
dr Joanna Przybylska, CGAP, MPA
Iwona Bogucka, EMPA, EMBA, DBA, LL.D.

O Instytucie Audytorów Wewnętrznych

Instytut Audytorów Wewnętrznych (The Institute of Internal Auditors - IIA) to międzynarodowe stowarzyszenie zawodowe, które zrzesza ponad 255 000 członków na całym świecie i przyznało ponad 200 000 certyfikatów Certified Internal Auditor® (CIA®) na całym świecie. Założona w 1941 r. organizacja IIA jest uznawana na całym świecie za lidera w zakresie standardów, certyfikacji, edukacji, badań i wytycznych technicznych w dziedzinie audytu wewnętrznego. Więcej informacji można znaleźć na stronie www.theiia.org.

Prawa autorskie

Maj 2025 r.