SYLABUS PROGRAMU, EDYCJA 2027

Akademia Zarządzania Cyberbezpieczeństwem

Praktyczny program dla małych i średnich firm, które nie mają specjalisty od cyberbezpieczeństwa i chcą przygotować własną osobę do pełnienia tej funkcji.

18 spotkań online na żywo po 2 godziny, dwa razy w tygodniu	**36 godzin** zajęć, w każdym spotkaniu ćwiczenia w małych grupach	**do 15 osób** w grupie, praca w podgrupach
10 tygodni 8 tygodni modułów, przerwa na projekt, obrony	**3 konsultacje** indywidualne z opiekunem projektu	**marzec 2027** planowany start, zapisy otwarte

IS Consulting sp. z o.o.
ul. Żelazna 51/53, 00-841 Warszawa | isconsulting.pl | events@isconsulting.pl
Wersja 1.0, 16 listopada 2026

1. Informacje podstawowe

Akademia w 10 tygodni przygotowuje osobę z małej lub średniej firmy do pełnienia funkcji osoby odpowiedzialnej za cyberbezpieczeństwo. Program prowadzi od pytania, co może zatrzymać albo okraść firmę, do kwartalnego raportu dla zarządu.

Pozycja	Informacja
Organizator	IS Consulting sp. z o.o., ul. Żelazna 51/53, 00-841 Warszawa, NIP 5273229833
Rodzaj programu	Praktyczny program szkoleniowy dla firm, skupiony na jednej roli.
Edycja i start	Edycja 2027, planowany start w marcu 2027
Czas trwania	10 tygodni: 8 tygodni modułów, tydzień przerwy na dokończenie projektu, tydzień obron
Zajęcia	18 spotkań online na żywo po 2 godziny, dwa razy w tygodniu, w godzinach pracy
Wymiar	36 godzin zajęć, 3 konsultacje indywidualne po 30 minut, około 2 godzin pracy nad projektem tygodniowo
Forma	Microsoft Teams, praca w podgrupach. Spotkań nie nagrywamy
Grupa	Do 15 osób
Język	Polski
Ukończenie	Numerowane zaświadczenie o ukończeniu programu, po obronie projektu
Zapisy	Formularz na stronie isconsulting.pl/uslugi/akademia, pytania: events@isconsulting.pl

2. Dla kogo jest Akademia

Akademia jest dla osoby, która w swojej firmie ma przejąć odpowiedzialność za cyberbezpieczeństwo, także bez doświadczenia w tej dziedzinie. Jest też dla osób, które już mają ten obowiązek, ale nikt ich do niego nie przygotował.

Typowo są to: kierownik IT lub administrator, kierownik administracji lub finansów, pełnomocnik do spraw jakości, inspektor ochrony danych albo członek zarządu małej firmy. Program jest przeznaczony dla firm zatrudniających od kilkudziesięciu do 250 osób, niezależnie od branży i od tego, czy firma podlega ustawie o krajowym systemie cyberbezpieczeństwa.

Wymagania wstępne

1. Wiedza techniczna nie jest potrzebna. Wystarczy ogólna orientacja w tym, jak działa firma i jej IT.
2. Zgoda pracodawcy na udział w zajęciach w godzinach pracy.
3. Około 6 godzin tygodniowo przez cały program: 4 godziny zajęć i około 2 godzin pracy nad projektem.

Czego Akademia nie robi

- **Nie jest kursem technicznym.** Nie uczy administracji systemami ani testów penetracyjnych. Absolwent stawia wymagania dostawcy IT i sprawdza ich realizację.
- **Nie jest kursem o przepisach.** Przepisy omawiamy tam, gdzie wynikają z ryzyka i dotyczą firmy, a nie dla nich samych.
- **Nie wykonuje pracy w firmie uczestnika.** Przygotowuje osobę, która ją wykona, ćwicząc na firmach przykładowych zamiast na danych własnej firmy.

3. Cel programu i efekty uczenia się

Celem programu jest przygotowanie osoby do samodzielnego pełnienia funkcji, a nie wykonanie części pracy w jej firmie. Każdy efekt jest sprawdzany w konkretnym etapie projektu albo na obronie.

Kod	Po programie absolwent potrafi	Moduły	Jak sprawdzamy
E01	Wskazać, co realnie może zatrzymać albo okraść firmę, i zaproponować zarządowi priorytety oraz budżet	1, 3	Etap 1, etap 2, obrona
E02	Ustalić, czego wymagają od firmy klienci, ubezpieczyciel, umowy i przepisy, w tym czy firma podlega ustawie o KSC	1	Etap 1
E03	Opisać, co musi działać, żeby firma działała, i wskazać punkty, których awaria zatrzymuje całą firmę	2	Etap 1
E04	Postawić dostawcy IT konkretne wymagania i sprawdzać, czy je spełnia	3, 6	Etap 3
E05	Wprowadzić krótkie zasady, które ludzie naprawdę stosują, i pokazać dowodami, że zabezpieczenia działają	4	Etap 3
E06	Poprowadzić firmę przez pierwsze godziny incydentu i dotrzymać obowiązujących terminów zgłoszeń	5	Ćwiczenie sztabowe, etap 3
E07	Sprawdzić, czy kopie zapasowe pozwolą firmie wrócić do pracy w akceptowalnym czasie	5	Etap 3
E08	Odpowiedzieć na ankietę klienta albo kwestionariusz ubezpieczyciela bez deklaracji, których nie da się udowodnić	4, 6	Etap 3
E09	Zaplanować działania budujące świadomość pracowników, zwłaszcza tam, gdzie firma traci pieniądze na oszustwach	7	Plan końcowy
E10	Regularnie raportować zarządowi stan bezpieczeństwa i decyzje do podjęcia	8	Plan końcowy, obrona

4. Metodyka

Akademia to praktyka pod okiem prowadzących, a nie cykl wykładów. Każde dwugodzinne spotkanie ma ten sam układ: krótka część merytoryczna z przykładami, ćwiczenie w małych grupach i zadanie do projektu na kolejne zajęcia.

- **Firmy przykładowe.** Ćwiczymy na fikcyjnych firmach opartych na realnych sytuacjach, na przykład sieci przychodni czy biurze rachunkowym. Nikt nie ujawnia zabezpieczeń własnej firmy, a prowadzący oceniają wszystkie prace według tych samych kryteriów.
- **Projekt od początku do końca.** Przez cały program uczestnik buduje plan zarządzania cyberbezpieczeństwem dla firmy przykładowej. Każdy moduł dokłada do niego kolejną część. Każdy uczestnik dostaje własny wariant firmy, z kilkoma innymi faktami, więc projekty się nie powielają.
- **Informacja zwrotna i konsultacje.** Prowadzący oceniają na piśmie każdy z trzech etapów projektu. Opiekun projektu prowadzi z uczestnikiem trzy konsultacje po 30 minut.
- **Ćwiczenie sztabowe.** W module 5 grupa przechodzi atak ransomware w czterech turach, z decyzjami pod presją czasu i komunikacją kryzysową.
- **Obrona.** Na koniec uczestnik przedstawia plan panelowi, który pyta jak zarząd decydujący o budżecie i jak klient proszący o dowody.
- **Mała grupa.** Do 15 osób, żeby każdy miał czas na pytania, dyskusję i pracę w podgrupach.
- **Materiały.** Po każdym spotkaniu uczestnik dostaje slajdy w PDF, kartę pracy i opis zadania do projektu.

5. Program

Osiem modułów obejmuje 16 spotkań (32 godziny), a dwa ostatnie spotkania (4 godziny) to obrony projektów. Każdy moduł kończy się ćwiczeniem i kolejną częścią projektu.

Moduł 1. Cyberbezpieczeństwo jako ryzyko biznesowe 2 spotkania, 4 h

- Jak naprawdę atakuje się małe i średnie firmy: oszustwo na podmieniony rachunek i „na prezesa", przejęcie poczty w Microsoft 365, ransomware, incydent u dostawcy.
- Ile kosztuje incydent: przestój, utracone zamówienia, odpowiedzialność wobec klientów, czas zarządu, wyższa składka ubezpieczeniowa.
- Rola osoby odpowiedzialnej: co należy do zarządu, co do niej, a co do dostawcy IT.
- Skąd przychodzą wymagania: klienci, ubezpieczyciele, przetargi, RODO, ustawa o KSC. Jak sprawdzić, czy firma podlega ustawie.

Ćwiczenie: które ataki zatrzymałyby firmę ćwiczeniową na dłużej niż dzień i kto w niej za co odpowiada.
W projekcie: opis zagrożeń i wymagań dla firmy przykładowej oraz podział odpowiedzialności.

Moduł 2. Usługi, systemy i zależności 1 spotkanie, 2 h

- Od usług do systemów: co musi działać, żeby firma sprzedawała.
- Ile szczegółu wystarczy w rejestrze i skąd wziąć dane.
- Zależności i punkty pojedynczej awarii: dostawcy, chmura, łącza, kluczowe osoby, wiedza w jednej głowie.
- Narzędzia używane poza wiedzą IT, w tym narzędzia AI.

Ćwiczenie: mapa zależności firmy ćwiczeniowej.
W projekcie: rejestr usług i systemów z mapą zależności.

Moduł 3. Ryzyko, priorytety i budżet 3 spotkania, 6 h

- Ryzyko w języku firmy: skutek finansowy, przestój, dane, klienci, wymagania zewnętrzne.
- Osiem scenariuszy, które najczęściej dotyczą małych i średnich firm, i jak je ocenić.
- Co zrobić z ryzykiem: ograniczyć, ubezpieczyć, uniknąć albo świadomie zaakceptować. Kto o tym decyduje.
- Minimum techniczne, którego trzeba wymagać od IT, i proporcjonalne zestawy zabezpieczeń dla małych firm.
- Priorytety i budżet na dwa kwartały oraz jak przedstawić je zarządowi.

Ćwiczenie: ocena scenariuszy, porównanie zabezpieczeń z kwestionariuszem ubezpieczyciela, wybór priorytetów z szacunkiem kosztu.
W projekcie: analiza ryzyka, priorytety i budżet.

Moduł 4. Zasady i dowody 2 spotkania, 4 h

- Jaki minimalny zestaw zasad wystarczy firmie i dlaczego kupione szablony częściej szkodzą, niż pomagają.
- Dostęp i uprawnienia, odejścia pracowników, kopie zapasowe, aktualizacje, szyfrowanie, płatności i zmiana danych kontrahenta, praca zdalna.
- Bezpieczne korzystanie z narzędzi AI w firmie: co wolno, czego nie wklejać, jak chronić dane.
- Co jest dowodem, że zabezpieczenie działa, i jak przygotować się na audyt klienta, pytania ubezpieczyciela albo kontrolę.

Ćwiczenie: luka w uprawnieniach przy odejściu pracownika, „dowód czy deklaracja”, odpowiedź na pytania z ankiety szpitala.
W projekcie: lista zasad do wprowadzenia i kalendarz dowodów.

Moduł 5. Incydenty i ciągłość działania 3 spotkania, 6 h

- Pierwsza godzina incydentu: kto decyduje, czego nie robić, jak współpracować z dostawcą IT.
- Oszustwo na rachunek: co zrobić z bankiem w pierwszych godzinach.
- Zgłoszenia: UODO, ubezpieczyciel, policja, klienci, a w firmach objętych ustawą o KSC także CSIRT.
- Jak długo firma wytrzyma przestój i czy kopie zapasowe na to pozwalają. Dlaczego tylko test odtworzenia dowodzi, że kopia działa.
- Ćwiczenie sztabowe: atak ransomware w czterech turach, z decyzjami pod presją czasu i komunikacją kryzysową.

Ćwiczenie: kwalifikacja zdarzeń, zestawienie wymagań ciągłości z raportem z kopii, ćwiczenie sztabowe.
W projekcie: procedura obsługi incydentu, wymagania ciągłości i plan testów odtworzenia.

Moduł 6. Dostawcy, chmura i dostawca IT 2 spotkania, 4 h

- Którzy dostawcy są krytyczni i jak ich ocenić. Co wynika z certyfikatów i raportów dostawcy, a czego nie dowodzą.
- Chmura i Microsoft 365: za co odpowiada dostawca, a co zostaje po stronie firmy.
- Wymagania bezpieczeństwa w umowach i powierzenie danych osobowych.
- Co dostawca IT powinien raportować co miesiąc i jak z nim rozmawiać bez wiedzy technicznej.
- Firma jako dostawca: odpowiadanie na ankiety klientów i kwestionariusze ubezpieczycieli.

Ćwiczenie: ocena dostawców, analiza umowy serwisowej, odpowiedź na kwestionariusz ubezpieczyciela.
W projekcie: lista dostawców krytycznych, wymagania wobec dostawcy IT i odpowiedź na ankietę.

Moduł 7. Ludzie: świadomość, oszustwa, komunikacja 1 spotkanie, 2 h

- Program świadomości: kogo uczyć, czego, jak często i jak mierzyć efekt.
- Socjotechnika w praktyce: podmieniony rachunek, polecenie „od prezesa”, fałszywy dział IT, telefon „z banku”.
- Kultura zgłaszania, w której pracownik nie boi się przyznać do kliknięcia.
- Jak komunikować zmiany, które pracownikom się nie spodobają.

Ćwiczenie: komunikat o wprowadzeniu uwierzytelniania wieloskładnikowego i rozmowa z księgowością o weryfikacji rachunków.
W projekcie: roczny plan świadomości i komunikacji.

Moduł 8. Nadzór: mierniki, cele i raport dla zarządu 2 spotkania, 4 h

- Co zarząd powinien zatwierdzać i jak często.
- Mierniki, które mają źródło danych, i raport kwartalny na jedną stronę.
- Dlaczego podstawowe zabezpieczenia nie są celem ambitnym i co trafia do celów kwartalnych.

Ćwiczenie: mierniki i raport dla firmy ćwiczeniowej, cel na kwartał z kluczowymi rezultatami.
W projekcie: mierniki, cele na dwa kwartały i struktura raportu dla zarządu.

Obrony projektów 2 spotkania, 4 h

Każdy uczestnik przedstawia plan dla swojej firmy przykładowej: 8 minut prezentacji i 5 minut pytań panelu. Na zakończenie podsumowujemy program i omawiamy, jak przenieść przećwiczoną metodę do własnej firmy.

6. Harmonogram

Program trwa 10 tygodni: osiem tygodni modułów po dwa spotkania, tydzień przerwy na dokończenie projektu i tydzień obron. Dni tygodnia i godziny spotkań podamy zgłoszonym osobom przed startem grupy.

Tydzień	1	2	3	4	5	6	7	8	9	10
Moduły	**M1**	**M2**	**M3**	**M4**	**M5**	**M6**	**M7**	**M8**	*Przerwa*	**Obrony**
Projekt		◆ Etap 1		◆ Etap 2			◆ Etap 3		◆ Plan końcowy	
Konsultacje			● K1			● K2			● K3	

Etapy projektu oddaje się na koniec tygodni 2, 4 i 7, plan końcowy w tygodniu przerwy, a konsultacje indywidualne (K1 do K3) wypadają w tygodniach 3, 6 i 9.

Spotkanie	Tydzień	Moduł	Temat spotkania
1	1	M1	Jak atakuje się małe i średnie firmy i ile kosztuje incydent
2	1	M1	Rola osoby odpowiedzialnej i źródła wymagań, w tym ustawa o KSC
3	2	M2	Usługi, systemy, zależności i punkty pojedynczej awarii
4	2	M3	Ryzyko w języku firmy i osiem scenariuszy dla MŚP
5	3	M3	Postępowanie z ryzykiem i minimum techniczne wobec IT
6	3	M3	Priorytety i budżet na dwa kwartały dla zarządu
7	4	M4	Minimalny zestaw zasad, w tym korzystanie z narzędzi AI
8	4	M4	Dowody działania zabezpieczeń, audyt klienta i pytania ubezpieczyciela
9	5	M5	Pierwsza godzina incydentu, oszustwo na rachunek, zgłoszenia
10	5	M5	Ciągłość działania, kopie zapasowe i test odtworzenia
11	6	M5	Ćwiczenie sztabowe: ransomware w czterech turach
12	6	M6	Dostawcy krytyczni, chmura i Microsoft 365
13	7	M6	Umowy, raportowanie dostawcy IT, ankiety klientów i ubezpieczycieli
14	7	M7	Świadomość, socjotechnika i kultura zgłaszania
15	8	M8	Co zatwierdza zarząd, mierniki i raport kwartalny
16	8	M8	Cele kwartalne i domknięcie planu
Przerwa	9		Dokończenie planu końcowego, konsultacja K3
17	10	Obrony	Obrony projektów
18	10	Obrony	Obrony projektów, podsumowanie i przeniesienie metody do własnej firmy

7. Projekt, ocena i ukończenie

Projekt to plan zarządzania cyberbezpieczeństwem dla firmy przykładowej, budowany w trzech etapach i domykany obroną. Uczestnik wykonuje tę samą pracę, którą po Akademii wykona we własnej firmie.

Część projektu	Zakres	Moduły	Termin oddania
Etap 1	Zagrożenia i wymagania, podział odpowiedzialności, rejestr usług i systemów z mapą zależności	1, 2	Koniec tygodnia 2
Etap 2	Analiza ryzyka na scenariuszach, priorytety i budżet na dwa kwartały	3	Koniec tygodnia 4

Część projektu	Zakres	Moduły	Termin oddania
Etap 3	Zasady i kalendarz dowodów, procedura obsługi incydentu, wymagania ciągłości i plan testów odtworzenia, ocena dostawców, wymagania wobec dostawcy IT, odpowiedź na ankietę klienta albo kwestionariusz ubezpieczyciela	4, 5, 6	Koniec tygodnia 7
Plan końcowy	Program świadomości pracowników, mierniki, cele na dwa kwartały, raport dla zarządu, cały plan gotowy do obrony	7, 8	Koniec tygodnia 9

Po każdym etapie uczestnik dostaje pisemną informację zwrotną. Między etapami odbywa trzy konsultacje po 30 minut z opiekunem projektu, w tygodniach 3, 6 i 9.

Obrona

Uczestnik ma 8 minut na prezentację planu i 5 minut na pytania panelu. Panel pyta jak zarząd decydujący o budżecie i jak klient proszący o dowody. Ocenia przede wszystkim:

- spójność planu: od zagrożeń i zależności, przez ryzyko, do priorytetów i budżetu,
- proporcjonalność do wielkości i realiów firmy przykładowej,
- oparcie odpowiedzi na dowodach, a nie na deklaracjach,
- wykonalność w dwóch kwartałach, z właścicielami zadań i kosztem,
- język zrozumiały dla zarządu: skutek dla firmy i decyzje do podjęcia.

Warunki ukończenia

1. Udział w co najmniej 15 z 18 spotkań.
2. Oddanie trzech etapów projektu.
3. Obrona planu końcowego.

Absolwent dostaje numerowane zaświadczenie o ukończeniu programu. Zaświadczenie potwierdza ukończenie programu i nie jest certyfikatem kompetencji w rozumieniu ISO/IEC 17024 ani uprawnieniem do audytu z art. 15 ustawy o KSC.

8. Zespół prowadzący

Zajęcia prowadzą praktycy, którzy na co dzień zajmują się zarządzaniem bezpieczeństwem, audytem i komunikacją. Skład prowadzących ogłosimy przed startem grupy.

Rola	Zadania
Prowadzący moduły	Część merytoryczna, prowadzenie ćwiczeń w podgrupach, pisemna ocena etapów projektu
Opiekun projektu	Trzy konsultacje indywidualne z każdym uczestnikiem, prowadzenie projektu od etapu 1 do obrony
Panel obron	Pytania z perspektywy zarządu i klienta, ocena planu końcowego

9. Zasady uczestnictwa

Zapisy są otwarte, a opłatę pobieramy dopiero po potwierdzeniu startu grupy. Grupę uruchamiamy po zebraniu wystarczającej liczby zgłoszeń, a liczba miejsc jest ograniczona do 15.

1. Zgłoszenie składa się przez formularz na stronie isconsulting.pl/uslugi/akademia, dla jednej lub kilku osób z firmy.
2. Przed uruchomieniem grupy przekazujemy wszystkim zgłoszonym osobom termin startu, harmonogram i warunki udziału, w tym zasady rezygnacji.
3. Po potwierdzeniu startu grupy wystawiamy fakturę. Ceny podajemy w złotych netto, z doliczonym VAT 23%.

Kilka osób z jednej firmy. Warunki ustalamy indywidualnie.

Nieobecność. Uczestnik dostaje slajdy i notatkę prowadzącego. Do ukończenia potrzebny jest udział w co najmniej 15 z 18 spotkań.

Wymagania techniczne. Komputer z dostępem do Microsoft Teams, głośnik i mikrofon. Kamera nie jest wymagana, ale ułatwia pracę w podgrupach.

Poufność. Pracujemy wyłącznie na firmach przykładowych. Uczestnik nie ujawnia informacji o zabezpieczeniach własnej firmy, a spotkań nie nagrywamy.

Materiały. Uczestnik może korzystać z materiałów na własny użytek zawodowy w swojej organizacji. Nie wolno ich rozpowszechniać ani utrwalać przebiegu zajęć.

10. Po Akademii

Absolwent wraca do firmy z przećwiczoną metodą i gotowym wzorem pracy: kompletnym planem dla firmy przykładowej, który obronił przed panelem. Ostatnie spotkanie poświęcamy temu, jak przenieść ten plan do własnej organizacji.

Absolwent staje się wewnętrznym właścicielem cyberbezpieczeństwa: koordynuje, pilnuje i raportuje zarządowi. Przy zadaniach specjalistycznych nadal warto korzystać z zewnętrznego wsparcia, ale firma będzie wiedziała, czego potrzebuje i jak sprawdzić efekt.