SZKOŁA BANKOWA W SANDOMIERZU

CENTRUM EDUKACYJNO-SZKOLENIOWE

STUDIA PODYPLOMOWE
„ZARZĄDZANIE BEZPIECZEŃSTWEM INFORMACJI I CYBERBEZPIECZEŃSTWEM W BANKOWOŚCI SPÓŁDZIELCZEJ”

Świadectwo ukończenia studiów z Uniwersytetu WSB MERITO we Wrocławiu

---

Rozpoczęcie: 24 PAŹDZIERNIKA 2026 R.

Studia obejmują 160 godzin dydaktycznych, **10 spotkań ONLINE (platforma Clickmeeting)**
po 2 dni (sobota - niedziela) zasadniczo 1 raz w miesiącu.
Koszt: 380 zł brutto za każde spotkanie + 600 zł brutto- opłata jednorazowa.

Proponowana metodyka łączy wymagania prawne, organizacyjne i techniczne z praktyką funkcjonowania Banku Spółdzielczego. Program został zaprojektowany tak, aby Uczestnik rozumiał nie tylko pojedyncze wymagania, lecz także zależności między nimi i potrafił przełożyć je na działania wykonywane w Banku.

Każdy blok programowy obejmuje część wykładową oraz ćwiczeniową. Zajęcia praktyczne mogą być prowadzone na przykładach dokumentów, rejestrów, scenariuszy i wyników testów spotykanych w bankowości spółdzielczej, z zachowaniem neutralności technologicznej i możliwości dostosowania do środowiska Uczestników.

PROGRAM OPARTY NA PRAKTYCZNEJ ŚCIEŻCE WDROŻENIA

Program studiów został zbudowany jako logiczny przewodnik po wdrażaniu najważniejszych aktualnych wymagań dotyczących bezpieczeństwa informacji, cyberbezpieczeństwa i odporności cyfrowej Banku Spółdzielczego.

Uczestnik przechodzi przez cały proces:
proces Banku → BIA → krytyczność → RTO/RPO/MTPD → system ICT → ZDU → umowa/SLA → ryzyko ICT → zabezpieczenia → BCM/DRP → incydent → test odporności → działanie naprawcze → raport dla Zarządu.
Dzięki temu poznaje nie tylko wymagania regulacyjne, ale przede wszystkim sposób ich praktycznego przełożenia na dokumentację, procesy, testy, dowody i decyzje podejmowane w Banku.

Szczególnie istotne elementy metodyki:

- **BIA a parametry umów z ZDU.** Analiza relacji pomiędzy RTO/RPO/MTPD wynikającymi z BIA a SLA, KPI i KRI określonymi w umowach. Program obejmuje identyfikację rozbieżności, ocenę ich wpływu na ryzyko oraz możliwe mechanizmy kompensacyjne w sytuacji, gdy dostosowanie parametrów umownych nie jest możliwe lub jest niewspółmierne.
- **Pełny cykl zarządzania ZDU.** Zakres obejmuje kwalifikację usługi i umowy, ocenę ryzyka, wymagania kontraktowe, SLA/KPI/KRI, Exit Plan, Strategię Wyjścia, monitoring, okresową ocenę oraz raportowanie do Zarządu w ramach systemu informacji zarządczej.

- **Testowanie odporności ICT jako system.** Program łączy testy własne IT, wyniki SOC/VM, niezależne testy podatności, testy penetracyjne i Threat Intelligence z jednym procesem klasyfikacji ustaleń, działań naprawczych, retestów i raportowania do Zarządu.
- **BIA Matryca Funkcji Kontroli.** Procesy BIA są powiązane z ryzykami, mechanizmami kontrolnymi, właścicielami, dowodami i testami, co pozwala przejść od identyfikacji procesu i ryzyka do weryfikacji adekwatności i skuteczności kontroli.

Wartością dla Uczestnika jest możliwość przełożenia omawianych zagadnień na działania, które mogą być wykorzystane w codziennej pracy w Banku: od przygotowania i weryfikacji BIA, przez ocenę ZDU i ryzyka ICT, po organizację testów, obsługę incydentu, działania naprawcze i przygotowanie informacji dla Zarządu.

WARTOŚĆ DLA UCZESTNIKA

- Poznanie zależności pomiędzy procesami biznesowymi, środowiskiem ICT, dostawcami i wymaganiami odporności;
- Umiejętność weryfikacji, czy dokumentacja Banku odpowiada rzeczywistym możliwościom technicznym i organizacyjnym;
- Praktyczne podejście do BIA, ryzyka ICT, ZDU, BCM/DRP, incydentów i testowania odporności;
- Umiejętność interpretowania wyników testów bezpieczeństwa oraz przekładania ich na działania naprawcze i ryzyko;
- Przygotowanie do współpracy pomiędzy Zarządem, IT, bezpieczeństwem, ryzykiem, compliance, audytem, IOD i ZDU;
- Umiejętność budowania spójnej informacji zarządczej o bezpieczeństwie i odporności ICT Banku.

Wiedza do wykorzystania w Banku

W trakcie studiów Uczestnicy poznają praktyczne podejście m.in. do:

- BIA i krytyczności procesów,
- analizy ryzyka ICT,
- zarządzania ZDU i umowami,
- BCM/DRP i testów odtworzeniowych,
- incydentów i naruszeń,
- testowania odporności, VA i pentestów,
- działań naprawczych,
- raportowania ryzyka i bezpieczeństwa ICT do Zarządu.

To program dla osób, które mają nie tylko znać wymagania, ale potrafić je wdrożyć, zweryfikować i zastosować w rzeczywistym środowisku Banku Spółdzielczego.

ADRESACI STUDIÓW

Studia są kierowane w szczególności do osób, które w Bankach Spółdzielczych odpowiadają za decyzje, nadzór lub realizację zadań w obszarze bezpieczeństwa informacji i odporności cyfrowej:

- Członków Zarządów oraz kadry kierowniczej;

- Pracowników IT, administratorów i osób odpowiedzialnych za cyberbezpieczeństwo;
- Pracowników ryzyka, compliance, kontroli wewnętrznej i audytu;
- Osób odpowiedzialnych za BIA, BCM/DRP i ciągłość działania;
- Osób nadzorujących ZDU, outsourcing i umowy ICT;
- IOD i osób uczestniczących w obsłudze incydentów oraz naruszeń danych;
- Pracowników przygotowywanych do objęcia nowych obowiązków w obszarze bezpieczeństwa i DORA.

PROWADZĄCY – PRAKTYCY BANKOWOŚCI SPÓŁDZIELCZEJ

Zajęcia prowadzą specjaliści **Servus Comp Kraków**, od wielu lat wspierający Banki Spółdzielcze w obszarze DORA, bezpieczeństwa informacji, cyberbezpieczeństwa, ryzyka ICT, BIA, ciągłości działania, ZDU, audytów oraz testowania operacyjnej odporności cyfrowej.

Program został oparty na doświadczeniach wynikających z **wieloletniej, bezpośredniej pracy z Bankami Spółdzielczymi** – przy wdrażaniu wymagań regulacyjnych, opracowywaniu i przeglądzie dokumentacji, analizach ryzyka, audytach, ocenie dostawców, organizacji testów oraz weryfikacji rzeczywistego środowiska ICT.

Servus Comp od lat prowadzi również dedykowane szkolenia dla Banków Spółdzielczych **we współpracy ze Szkołą Bankową w Sandomierzu,** co pozwala łączyć doświadczenie wdrożeniowe z praktyką szkoleniową i znajomością realnych potrzeb pracowników tego sektora.

FORMA I ORGANIZACJA STUDIÓW

Studia prowadzone są w całości **online (platforma Clickmeeting),** w czasie rzeczywistym, w układzie 10 dwudniowych spotkań weekendowych, realizowanych zasadniczo raz w miesiącu.

Program obejmuje:

- 160 godzin dydaktycznych;
- 68 godzin wykładów;
- 92 godziny ćwiczeń, warsztatów i symulacji;
- 10 bloków programowych;
- 10 dwudniowych spotkań online;
- 16 godzin dydaktycznych podczas każdego spotkania;
- 8 godzin w sobotę i 8 godzin w niedzielę.

Dla bloków o podziale 8/8 proponuje się po 4 godziny wykładu i 4 godziny ćwiczeń w każdym dniu. Dla bloków o podziale 4/12 proponuje się po 2 godziny wykładu i 6 godzin ćwiczeń w każdym dniu. Pozwala to zachować 8-godzinny dzień zajęć oraz łączny podział 68 godzin wykładów i 92 godziny ćwiczeń.

PODSTAWA MERYTORYCZNA I ODNIESIENIA

Zakres merytoryczny poszczególnych bloków może być odnoszony w szczególności do następujących regulacji, standardów i dobrych praktyk:

- Rozporządzenie (UE) 2022/2554 (DORA) – zarządzanie ryzykiem ICT, incydenty, testowanie odporności i ryzyko dostawców ICT;
- Rozporządzenie delegowane Komisji (UE) 2024/1774 – narzędzia, metody, procesy i polityki zarządzania ryzykiem ICT;
- Rozporządzenie delegowane Komisji (UE) 2024/1773 – polityka dotycząca umów na usługi ICT wspierające funkcje krytyczne lub istotne;
- Rozporządzenie delegowane Komisji (UE) 2024/1772 – klasyfikacja incydentów ICT, progi istotności i informacje dotyczące raportowania poważnych incydentów;
- RODO – Rozporządzenie (UE) 2016/679;
- NIS2 oraz ustawa o krajowym systemie cyberbezpieczeństwa w obowiązującym brzmieniu;
- ISO/IEC 27001 – system zarządzania bezpieczeństwem informacji;
- ISO/IEC 27005 i ISO 31000 – zarządzanie ryzykiem;
- ISO 22301 – ciągłość działania;
- ISO 19011 – zasady audytowania systemów zarządzania;
- Wewnętrzne regulacje Banku, wymagania zrzeszenia oraz obowiązujące wytyczne sektorowe – odpowiednio do organizacji Uczestnika.

CEL METODYKI

Celem jest przygotowanie Uczestnika do rozumienia i łączenia wymagań organizacyjnych z rzeczywistym środowiskiem ICT Banku. Poszczególne bloki zostały ułożone tak, aby tworzyły logiczny ciąg: **proces i krytyczność → wymagane parametry odporności → usługi i dostawcy → ryzyko ICT → zabezpieczenia i ciągłość → incydenty → testowanie → audyt i dowody → informacja zarządcza.**

PROGRAM STUDIÓW

Lp.	Blok programowy	Wykłady	Ćwiczenia	Razem
1	**BIA i zarządzanie krytycznością procesów**	8	8	16
2	**Spójność BIA z parametrami usług, umowami ICT i ZDU**	8	8	16
3	**Analiza i zarządzanie ryzykiem ICT, aktywami i compliance**	8	8	16
4	**System zarządzania bezpieczeństwem informacji i bezpieczeństwo środowiska ICT**	8	8	16
5	**Ciągłość działania, BCM/DRP i odporność środowiska ICT**	8	8	16
6	**Zarządzanie incydentami ICT, cyberincydentami i ochroną danych**	4	12	16
7	**Testowanie operacyjnej odporności ICT i zarządzanie wynikami testów**	4	12	16
8	**Audyt bezpieczeństwa, funkcja kontroli i informatyka śledcza**	8	8	16
9	**OSINT, socjotechnika, cyberoszustwa i Threat Intelligence**	8	8	16
10	**Zarządzanie kryzysowe, raportowanie do Zarządu i symulacja końcowa**	4	12	16

Lp.	Blok programowy	Wykłady	Ćwiczenia	Razem
	RAZEM	**68**	**92**	**160**

ZAKRES TEMATYCZNY I PODZIAŁ NA DNI

1. BIA i zarządzanie krytycznością procesów (8 h wykładów / 8 h ćwiczeń)

- **Sobota:** rola BIA w zarządzaniu odpornością Banku;
- BIA – Wytyczne BIA; BIA – Księga Procesów; BIA – Analiza Krytyczności Procesów; BIA – Matryca Funkcji Kontroli;
- identyfikacja procesów, właścicieli i zależności;
- RTO, RPO, MTPD/MAO oraz zasady ich wyznaczania.
- **Niedziela:** warsztat budowy fragmentu Księgi Procesów i analizy krytyczności;
- mapowanie procesu na systemy ICT, dane, personel, lokalizacje i ZDU;
- powiązanie procesów z ryzykami, mechanizmami kontrolnymi, właścicielami, dowodami i testami;
- ocena spójności parametrów BIA z rzeczywistą zdolnością operacyjną Banku.
- **Odniesienia:** DORA; RTS 2024/1774; ISO 22301; ISO 27001; ISO 31000.

2. Spójność BIA z parametrami usług, umowami ICT i ZDU (8 h wykładów / 8 h ćwiczeń)

- **Sobota:** relacje pomiędzy RTO/RPO/MTPD/MAO a SLA, KPI i KRI;
- mapowanie procesów BIA na usługi ICT i konkretne umowy;
- klasyfikacja usług i umów: funkcje krytyczne lub istotne oraz pozostałe usługi;
- ocena, czy parametry umowne wspierają wymagania wynikające z BIA.
- **Niedziela:** analiza rozbieżności pomiędzy BIA i umową;
- metody kompensacji, gdy dostosowanie parametrów umownych jest niewykonalne;
- Exit Plan i Strategia Wyjścia;
- monitoring ZDU, okresowa ocena, SLA/KPI/KRI i raportowanie do Zarządu w ramach SIZ.
- **Odniesienia:** DORA, w szczególności obszar ryzyka dostawców ICT; RTS 2024/1773; RTS 2024/1774; ISO 22301; ISO 31000.

3. Analiza i zarządzanie ryzykiem ICT, aktywami i compliance (8 h wykładów / 8 h ćwiczeń)

- **Sobota:** kompleksowa analiza ryzyka środowiska ICT Banku;
- identyfikacja aktywów, zagrożeń, podatności i zabezpieczeń;
- ryzyko inherentne i rezydualne, właściciele ryzyka i plany postępowania;
- rejestr ryzyka ICT, apetyt/tolerancja na ryzyko oraz powiązanie z BIA.
- **Niedziela:** inwentaryzacja aktywów ICT i CMDB/rejestr aktywów;
- zarządzanie zmianą i wpływem zmian na ryzyko oraz procesy krytyczne;
- compliance i kontrola wewnętrzna w obszarze ICT;
- warsztat aktualizacji oceny ryzyka po incydencie, zmianie technologicznej lub zmianie ZDU.
- **Odniesienia:** DORA; RTS 2024/1774; ISO/IEC 27005; ISO 31000; ISO/IEC 27001.

4. System zarządzania bezpieczeństwem informacji i bezpieczeństwo środowiska ICT (8 h wykładów / 8h ćwiczeń)

- **Sobota:**
- SZBI według ISO/IEC 27001 i organizacja bezpieczeństwa informacji w Banku;
- role, odpowiedzialności i podział kompetencji w obszarze bezpieczeństwa informacji, cyberbezpieczeństwa i ochrony danych;
- ochrona informacji i danych osobowych w procesach Banku – klasyfikacja informacji, zasady dostępu, poufność i minimalizacja uprawnień;
- podstawowe obowiązki wynikające z RODO, DORA oraz regulacji dotyczących cyberbezpieczeństwa, w tym KSC/NIS2 – w zakresie właściwym dla Banku;

- powiązanie bezpieczeństwa informacji z ryzykiem ICT, ochroną danych oraz regulacjami wewnętrznymi Banku.
- **Niedziela:**
- współpraca z dostawcami usług ICT i ZDU z perspektywy bezpieczeństwa informacji i ochrony danych;
- wymagania bezpieczeństwa i ochrony danych w umowach, w tym powierzenie przetwarzania danych oraz obowiązki dotyczące podwykonawców;
- zasady nadzorowania dostawców, wymiany informacji o incydentach, podatnościach i zagrożeniach oraz oceny wpływu zdarzeń po stronie dostawcy na Bank;
- weryfikacja zgodności regulacji wewnętrznych, umów i rzeczywiście stosowanych rozwiązań organizacyjnych;
- warsztat: identyfikacja luk w dokumentacji bezpieczeństwa, ochrony danych i współpracy z dostawcami oraz określenie działań naprawczych.
- **Odniesienia:** DORA; RTS 2024/1774; RODO; ISO/IEC 27001; NIS2/KSC; regulacje wewnętrzne Banku.

5. Ciągłość działania, BCM/DRP i odporność środowiska ICT (8 h wykładów / 8 h ćwiczeń)

- **Sobota:** system zarządzania ciągłością działania;
- strategie ciągłości wynikające z BIA;
- BCP, DRP, procedury awaryjne i rozwiązania zastępcze;
- backup, odporność na ransomware, retencja kopii i zasady odtworzenia.
- **Niedziela:** testy odtworzeniowe oraz weryfikacja osiągniętych RTO/RPO;
- failover łączy, systemów i usług krytycznych;
- scenariusze awarii systemu centralnego, bankowości elektronicznej, łączności i ZDU;
- ocena rozbieżności pomiędzy planowanym a rzeczywistym czasem odtworzenia.
- **Odniesienia:** DORA; RTS 2024/1774; ISO 22301; ISO/IEC 27001.

6. Zarządzanie incydentami ICT, cyberincydentami i ochroną danych (4 h wykładów / 12 h ćwiczeń)

- **Sobota:**
- organizacja procesu zarządzania incydentami w Banku – od identyfikacji zdarzenia do zamknięcia incydentu;
- klasyfikacja i priorytetyzacja incydentów ICT oraz cyberincydentów;
- kryteria klasyfikacji incydentów na potrzeby DORA, w tym identyfikacja poważnych incydentów ICT;
- incydent ICT a naruszenie ochrony danych osobowych – zasady kwalifikacji i oceny ryzyka dla praw i wolności osób;
- role i odpowiedzialności IT, bezpieczeństwa, Zarządu, compliance, IOD, SOC i ZDU;
- eskalacja, rejestracja, dokumentowanie incydentu oraz uruchamianie właściwych ścieżek postępowania;
- powiązanie obsługi incydentu z BCM/DRP i komunikacją podczas incydentu.
- **Niedziela – warsztaty:**
- kwalifikacja zgłoszeń: zdarzenie / incydent / naruszenie ochrony danych;
- klasyfikacja przykładowych incydentów według DORA;
- ocena ryzyka naruszenia ochrony danych;
- ustalenie właściwej ścieżki eskalacji i osób, które należy zaangażować;
- decyzja, które procedury Banku należy uruchomić;
- przygotowanie wpisu do rejestru incydentów lub naruszeń;
- podjęcie i uzasadnienie decyzji dotyczącej zgłoszenia;
- przygotowanie podstawowej dokumentacji incydentu;
- analiza po incydencie i wskazanie działań naprawczych.
- **Odniesienia:** DORA; RTS 2024/1772; RODO; ISO/IEC 27001; ISO 22301.

7. Testowanie operacyjnej odporności ICT i zarządzanie wynikami testów (4 h wykładów / 12 h ćwiczeń)

- **Sobota:** cele, zakres i roczny program testów operacyjnej odporności ICT;
- testy podstawowe, zaawansowane, scenariuszowe i testy ZDU;
- testy własne podatności wykonywane przez IT, wyniki SOC/VM (np. Rapid7), niezależne VA i testy penetracyjne;
- role, odpowiedzialności, kryteria, dowody oraz raport z testu.

- **Niedziela:** warsztat budowy rocznego harmonogramu testów;
- agregacja wyników z różnych źródeł, deduplikacja i klasyfikacja ustaleń;
- właściciele, terminy, akceptacja ryzyka, działania naprawcze i retesty;
- jednolity rejestr ustaleń oraz raportowanie wyników i trendów do Zarządu.
- **Odniesienia:** DORA – ramy testowania operacyjnej odporności cyfrowej; RTS 2024/1774; ISO/IEC 27001; ISO 22301.

8. Audyt bezpieczeństwa, funkcja kontroli i informatyka śledcza (8 h wykładów / 8 h ćwiczeń)

- **Sobota:** zasady audytu według ISO 19011;
- program, plan, kryteria i dowody audytowe;
- badanie zgodności dokumentacji z rzeczywistym działaniem mechanizmów;
- BIA Matryca Funkcji Kontroli jako narzędzie powiązania procesów, ryzyk, mechanizmów, dowodów i testów.
- **Niedziela:** test adekwatności i skuteczności mechanizmów kontrolnych;
- zarządzanie niezgodnościami i działaniami naprawczymi;
- podstawy informatyki śledczej: zabezpieczanie dowodów, integralność, analiza logów i rekonstrukcja zdarzeń;
- warsztat raportowania ustaleń audytowych i śledzenia ich zamknięcia.
- **Odniesienia:** ISO 19011; ISO/IEC 27001; ISO 22301; DORA; RTS 2024/1774.

9. OSINT, socjotechnika, cyberoszustwa i Threat Intelligence (8 h wykładów / 8 h ćwiczeń)

- **Sobota:** OSINT i informacje publicznie dostępne o Banku;
- phishing, vishing, smishing, spoofing i kradzież tożsamości;
- cyberoszustwa w bankowości elektronicznej i manipulowanie pracownikami/klientami;
- Threat Intelligence / Cyber Threat Intelligence jako źródło informacji o zagrożeniach.
- **Niedziela:** warsztat identyfikacji ekspozycji informacyjnej Banku;
- analiza scenariuszy socjotechnicznych i oszustw;
- przekładanie informacji o zagrożeniach na analizę ryzyka, testy i działania zabezpieczające;
- budowanie programu świadomości bezpieczeństwa.
- **Odniesienia:** DORA; NIS2/KSC; ISO/IEC 27001; dobre praktyki cyberbezpieczeństwa sektora finansowego.

10. Zarządzanie kryzysowe, raportowanie do Zarządu i symulacja końcowa (4 h wykładów / 12 h ćwiczeń)

- **Sobota:** organizacja zespołu kryzysowego i rola Zarządu;
- podejmowanie decyzji pod presją czasu;
- komunikacja wewnętrzna, z klientami, ZDU i właściwymi instytucjami;
- raportowanie bezpieczeństwa ICT do Zarządu: ryzyka, incydenty, podatności, testy, ZDU, KPI/KRI i działania naprawcze.
- **Niedziela:** kompleksowa symulacja cyberincydentu w Banku Spółdzielczym;
- organizacja pracy zespołu kryzysowego i podział odpowiedzialności;
- analiza informacji napływających w trakcie sytuacji kryzysowej i podejmowanie decyzji;
- decyzje dotyczące komunikacji z klientami, ZDU i właściwymi instytucjami;
- przygotowanie informacji i komunikatów na potrzeby Zarządu oraz komunikacji zewnętrznej;
- zakończenie sytuacji kryzysowej i podsumowanie podjętych działań;
- wnioski dotyczące organizacji zarządzania kryzysowego i komunikacji.
- **Odniesienia:** DORA; RTS 2024/1772; RODO; ISO 22301; ISO/IEC 27001; ISO 19011.
- **KOŃCOWY TEST ZALICZENIOWY.**

METODY PROWADZENIA ZAJĘĆ

- Wykłady interaktywne online;
- Ćwiczenia i warsztaty na dokumentach i rejestrach;
- Analizy przypadków z realiów Banków Spółdzielczych;
- Ćwiczenia z BIA, oceny ryzyka, ZDU, incydentów i testowania odporności;
- Analiza raportów technicznych, wyników testów i dowodów;
- Ćwiczenia audytowe i analiza mechanizmów kontrolnych;
- Analiza logów i materiału dowodowego;
- Symulacje sytuacji kryzysowych oraz ćwiczenia decyzyjne dla Zarządu i zespołów operacyjnych;
- Zadania indywidualne i zespołowe.

Metodyka zakłada prowadzenie zajęć w sposób łączący wymaganie regulacyjne z dokumentem, procesem, konfiguracją lub działaniem operacyjnym, dowodem wykonania oraz sposobem weryfikacji skuteczności.

EFEKTY UCZENIA SIĘ

Po ukończeniu studiów Uczestnik:

- potrafi powiązać procesy Banku z ich krytycznością, parametrami BIA, systemami ICT i dostawcami;
- rozumie zależności pomiędzy wymaganiami BIA a SLA/KPI/KRI i potrafi identyfikować luki;
- potrafi uczestniczyć w analizie ryzyka ICT oraz ocenie ZDU i usług ICT;
- potrafi ocenić podstawowe mechanizmy bezpieczeństwa systemów, infrastruktury i dostępu;
- rozumie zasady BCM/DRP, backupu, odtwarzania i testowania ciągłości;
- potrafi uczestniczyć w klasyfikacji, obsłudze i raportowaniu incydentu ICT;
- rozumie sposób budowy programu testów odporności oraz zarządzania wynikami VA, SOC i pentestów;
- potrafi pracować z dowodami audytowymi, niezgodnościami i działaniami naprawczymi;
- rozpoznaje zagrożenia socjotechniczne, OSINT i znaczenie Threat Intelligence;
- potrafi przygotować syntetyczną informację zarządczą o ryzyku i odporności ICT Banku.

ZALICZENIE STUDIÓW

Warunki ukończenia studiów:

- uczestnictwo w zajęciach;
- wykonanie wymaganych ćwiczeń i zadań;
- udział w kompleksowej symulacji cyberincydentu;
- uzyskanie pozytywnego wyniku końcowego testu zaliczeniowego.

Końcowy test online składa się z **30 pytań jednokrotnego wyboru** i obejmuje zagadnienia przedstawione podczas studiów.

CERTYFIKACJA AUDYTORSKA

Program obejmuje zagadnienia przydatne w przygotowaniu merytorycznym do procesów certyfikacyjnych związanych z audytem ISO/IEC 27001 i ISO 22301. Uzyskanie właściwego certyfikatu audytorskiego pozostaje odrębnym procesem i zależy od wymagań jednostki certyfikującej.

RAZEM: 160 GODZIN
