EDUKACJA EKONOMISTÓW I MENEDŻERÓW
Nr 75–76(1–2), styczeń–czerwiec 2025

Artykuł nadesłany: 13 stycznia 2026; Poprawiony: 20 marca 2026; Zaakceptowany: 13 maja 2026

DOI: 10.33119/EEIM.2025.75-76.1

Markiewicz, I. (2025). Cyberbezpieczeństwo jako obszar odpowiedzialności kadry zarządzającej: od zgodności regulacyjnej do budowania odporności organizacyjnej. *Edukacja Ekonomistów i Menedżerów*, 75–76(1–2), 9–19.
Pobrane z: https://econjournals.sgh.waw.pl/EEiM/article/view/5458

Cyberbezpieczeństwo jako obszar odpowiedzialności kadry zarządzającej: od zgodności regulacyjnej do budowania odporności organizacyjnej

Izabela Markiewicz

Wydział Nauk Politycznych i Studiów Międzynarodowych,
Uniwersytet Warszawski

Wzrost skali i złożoności zagrożeń cyfrowych sprawia, że cyberbezpieczeństwo przestaje być domeną wyspecjalizowanych zespołów IT, a staje się obszarem odpowiedzialności kadry zarządzającej w szczególności w kontekście ładu organizacyjnego, zarządzania ryzykiem i ciągłości działania. W ostatnich latach odpowiedzialność ta została dodatkowo wzmocniona regulacyjnie: dyrektywa NIS2 nakłada na organy zarządzające obowiązek zatwierdzania i nadzorowania środków zarządzania ryzykiem cybernetycznym oraz przewiduje możliwość pociągnięcia ich do odpowiedzialności, a rozporządzenie DORA w sektorze finansowym akcentuje „pełną i ostateczną" odpowiedzialność organu zarządzającego za zarządzanie ryzykiem ICT i wymóg stałego podnoszenia kompetencji. Celem artykułu jest uporządkowanie zakresu tej odpowiedzialności poprzez zintegrowanie perspektywy regulacyjnej i normatywnej (NIS2, DORA, NIST CSF 2.0, ISO/IEC 27001 i ISO/IEC 27014) z dorobkiem naukowym w obszarze zarządzania bezpieczeństwem informacji. Na tej podstawie proponowany jest model „cyklu odpowiedzialności zarządczej" oraz zestaw praktyk wdrożeniowych obejmujących m.in. definiowanie apetytu na ryzyko,

alokację zasobów, nadzór nad łańcuchem dostaw ICT oraz budowanie kultury cyberbezpieczeństwa. Artykuł wskazuje także konsekwencje dla edukacji menedżerów i funkcji HR, w tym potrzebę instytucjonalizacji szkoleń dla członków organów zarządzających.

Słowa kluczowe: cyberbezpieczeństwo, odpowiedzialność zarządcza, ład organizacyjny, zarządzanie ryzykiem, NIS2, DORA

Kody klasyfikacji JEL: G34, M15, D81

Wprowadzenie

Cyfrowa transformacja obejmująca upowszechnienie chmury obliczeniowej, pracy zdalnej, automatyzacji procesów oraz intensyfikację wymiany danych w łańcuchach dostaw spowodowała, że ryzyko cybernetyczne stało się jednym z kluczowych ryzyk przedsiębiorstw i instytucji publicznych. Jego materializacja przekłada się na straty finansowe, zakłócenia operacyjne, utratę zaufania interesariuszy oraz konsekwencje prawne. W ujęciu makroekonomicznym cyberincydenty oddziałują na konkurencyjność i stabilność sektorów krytycznych, jest to widoczne w rosnącej aktywności regulatorów. Raport IBM wskazuje, że globalny średni koszt naruszenia danych w 2024 r. wzrósł rok do roku o 10% do 4,88 mln USD, a znaczącą część wzrostu kosztów generuje zakłócenie biznesu i działania po incydencie (IBM Security, 2024). Z kolei ENISA, analizując 4875 incydentów z okresu 1.07.2024–30.06.2025, podkreśla utrzymującą się różnorodność i konwergencję działań grup zagrożeń, a także powtarzalność technik i modeli ataku w UE (ENISA, 2025). W powyższych warunkach cyberbezpieczeństwo przestało być wyłącznie zagadnieniem technologicznym. Rosnąca rola ładu organizacyjnego w obszarze cyberprzestrzeni jest potwierdzana zarówno przez literaturę, która wskazuje na potrzebę włączenia bezpieczeństwa informacji do *corporate governance* (Posthumus, von Solms, 2004; von Solms, von Solms, 2006), jak i przez regulacje europejskie. Dyrektywa NIS2 zobowiązuje państwa członkowskie do zapewnienia, aby organy zarządzające podmiotów kluczowych i ważnych zatwierdzały środki zarządzania ryzykiem cybernetycznym, nadzorowały ich wdrożenie oraz mogły ponosić odpowiedzialność za naruszenia (UE, 2022a). Jednocześnie NIS2 wprost wymaga szkoleń dla członków organów zarządzających (UE, 2022a). W sektorze finansowym rozporządzenie DORA akcentuje „pełną i ostateczną odpowiedzialność" organu zarządzającego za zarządzanie ryzykiem ICT oraz obowiązek utrzymywania aktualnej wiedzy i umiejętności poprzez regularne szkolenia (UE, 2022b). W Polsce kierunek ten znajduje odzwierciedlenie w projektowanych zmianach ustawy o krajowym systemie cyberbezpieczeństwa, które według komunikatu Ministerstwa Cyfryzacji mają wzmocnić ochronę przed cyberzagrożeniami

i m.in. wprowadzić wymogi organizacyjne oraz szkoleniowe na poziomie kierownictwa (Ministerstwo Cyfryzacji, 2025).

Celem artykułu jest zdefiniowanie cyberbezpieczeństwa jako obszaru odpowiedzialności kadry zarządzającej, uporządkowanie tej odpowiedzialności w postaci modelu i mapy ról oraz wskazanie implikacji dla rozwoju kompetencji menedżerów, w tym dla programów edukacyjnych oraz praktyk HR. Artykuł ma charakter koncepcyjno-przeglądowy, oparty na analizie dokumentów regulacyjnych i normatywnych oraz literatury naukowej.

Metodyka: analiza dokumentów i przegląd literatury

Artykuł opiera się na zintegrowanym przeglądzie literatury oraz analizie treści dokumentów o charakterze regulacyjnym i normatywnym. Do analizy włączono w szczególności: dyrektywę NIS2 (UE, 2022a), rozporządzenie DORA (UE, 2022b), ramy zarządzania ryzykiem cybernetycznym NIST CSF 2.0 (NIST, 2024) oraz standardy rodziny ISO/IEC 27000, w tym ISO/IEC 27001 dotyczący systemów zarządzania bezpieczeństwem informacji (ISO, 2022). Dokumenty te zestawiono z dorobkiem naukowym dotyczącym bezpieczeństwa informacji, w tym z klasycznymi modelami integrującymi bezpieczeństwo informacji z *corporate governance* (Posthumus, von Solms, 2004; von Solms, von Solms, 2006) oraz nowszymi pracami akcentującymi odpowiedzialność rad nadzorczych i zarządów w warunkach ograniczonej ekspertyzy (Lowry i in., 2025; Harel, 2025).

Na podstawie analizy sformułowano model „cyklu odpowiedzialności zarządczej" oraz zestaw praktyk wdrożeniowych, które łączą perspektywę *compliance* (spełnienie wymagań) z perspektywą *resilience* (zdolność organizacji do utrzymania i odtworzenia krytycznych funkcji w warunkach zakłócenia).

Cyberbezpieczeństwo w logice ładu organizacyjnego i zarządzania ryzykiem

Z perspektywy nauk o zarządzaniu cyberbezpieczeństwo można traktować jako szczególny przypadek zarządzania ryzykiem operacyjnym, którego materializacja może mieć konsekwencje strategiczne (utrata rynku, reputacji, ograniczenie zdolności do świadczenia usług) oraz prawne. W literaturze dotyczącej bezpieczeństwa informacji podkreśla się, że najwyższy poziom zarządzania powinien nie tylko „wspierać" działania bezpieczeństwa, ale je współkształtować poprzez mechanizmy kierowania i nadzoru (Posthumus, von Solms, 2004). Model Direct Control Cycle

wskazuje na dwie komplementarne funkcje: „direct" (wyznaczanie kierunku) oraz „control" (kontrola i monitoring rezultatów), osadzone w cyklu ciągłego doskonalenia (von Solms, von Solms, 2006). Analogiczną logikę odnajdujemy w nowszych ramach zarządzania ryzykiem cybernetycznym. NIST CSF 2.0 wprowadza funkcję GOVERN jako równorzędną wobec IDENTIFY, PROTECT, DETECT, RESPOND i RECOVER, wskazując, że działania z obszaru *governance* muszą zachodzić równolegle z działaniami operacyjnymi i być gotowe „w każdej chwili" (NIST, 2024). ISO/IEC 27014 adresuje ład bezpieczeństwa informacji jako procesy oceny, ukierunkowania, monitorowania i komunikowania, ukierunkowane na interesariuszy i powiązane z ISMS (ISO, 2020). Z kolei ISO 31000 porządkuje ogólną logikę zarządzania ryzykiem (identyfikacja – analiza – ocena – postępowanie z ryzykiem – monitorowanie – komunikacja), co stanowi naturalny punkt odniesienia dla cyberryzyka jako elementu *enterprise risk management* (ISO, 2018). Wspólnym mianownikiem tych ujęć jest przesunięcie akcentu z „narzędzi" na „decyzje": cyberbezpieczeństwo staje się zbiorem decyzji o priorytetach, akceptowanym poziomie ryzyka, alokacji zasobów, architekturze odpowiedzialności oraz mechanizmach raportowania. Decyzje te zgodnie z logiką *corporate governance* powinny być podejmowane i nadzorowane przez kadrę zarządzającą, przy wykorzystaniu ekspertyzy wyspecjalizowanych ról (CISO, CIO, *compliance*, audyt), ale bez delegowania odpowiedzialności.

Regulacyjne umocowanie odpowiedzialności zarządczej: NIS2 i DORA

Regulacje europejskie precyzują elementy odpowiedzialności kadry zarządzającej w sposób, który istotnie wpływa na praktyki zarządcze. W NIS2 (art. 20) wskazano trzy kluczowe wątki: 1) zatwierdzenie przez organy zarządzające środków zarządzania ryzykiem cybernetycznym, 2) nadzór nad wdrożeniem oraz 3) możliwość pociągnięcia ich do odpowiedzialności za naruszenia (UE, 2022a). NIS2 wprowadza także wymóg szkoleń dla członków organów zarządzających, aby posiadali wiedzę umożliwiającą identyfikację ryzyk i ocenę praktyk zarządzania ryzykiem cyber (UE, 2022a). Jednocześnie art. 21 NIS2 kataloguje minimalne kategorie środków (m.in. obsługa incydentów, ciągłość działania, bezpieczeństwo łańcucha dostaw, kryptografia, szkolenia, MFA), co stanowi punkt odniesienia dla oczekiwań regulacyjnych wobec programów bezpieczeństwa (UE, 2022a).

W rozporządzeniu DORA odpowiedzialność ta została doprecyzowana dla sektora finansowego. Rozporządzenie akcentuje, że „pełna i ostateczna odpowiedzialność" organu zarządzającego za ryzyko ICT jest zasadą nadrzędną podejścia do odporności cyfrowej, a organ zarządzający ma aktywnie angażować się w kontrolę i monitoring

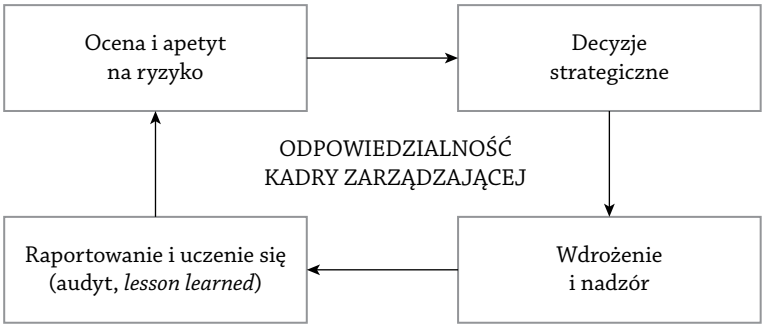
ram zarządzania ryzykiem ICT (UE, 2022b). W ujęciu operacyjnym DORA nakłada na organ zarządzający obowiązek definiowania, zatwierdzania, nadzorowania i ponoszenia odpowiedzialności za wdrożenie ram zarządzania ryzykiem ICT, w tym ustanawiania ról i odpowiedzialności oraz zapewnienia standardów dostępności, integralności i poufności danych (UE, 2022b). Rozporządzenie wymaga również, aby członkowie organu zarządzającego utrzymywali aktualną wiedzę i umiejętności poprzez regularne szkolenia adekwatne do zarządzanego ryzyka ICT (UE, 2022b). DORA znajduje zastosowanie od 17 stycznia 2025 r., co w praktyce wymuszało na podmiotach finansowych przyspieszenie programów *compliance* i podniesienie dojrzałości operacyjnej (UE, 2022b).

W Polsce, w ramach prac nad wdrożeniem NIS2, podkreśla się znaczenie wzmocnienia mechanizmów ochrony i odpowiedzialności kierownictwa w podmiotach kluczowych i ważnych, co ma przełożyć się na spójniejsze standardy organizacyjne, raportowanie incydentów oraz rozwój kompetencji (Ministerstwo Cyfryzacji, 2025).

Model cyklu odpowiedzialności zarządczej w cyberbezpieczeństwie

W oparciu o analizę regulacji, standardów oraz literatury proponuje się model „cyklu odpowiedzialności zarządczej" (rysunek 1).

Rysunek 1. Cykl odpowiedzialności zarządczej w cyberbezpieczeństwie



Źródło: opracowanie własne na podstawie: von Solms i von Solms (2006); NIST (2024); ISO (2020).

Model integruje perspektywę „Direct – Control Cycle" (von Solms, von Solms, 2006) z naciskiem na *governance* obecnym w NIST CSF 2.0 (NIST, 2024) oraz ISO/IEC 27014 (ISO, 2020). Zakłada on, że odpowiedzialność kadry zarządzającej realizuje się w powtarzalnym cyklu: 1) ocena i ustalenie apetytu na ryzyko, 2) decyzje strategiczne (polityki, budżet, priorytety), 3) wdrożenie i nadzór (programy, ISMS,

portfel projektów), 4) raportowanie i uczenie się (metryki, audyt, wnioski po incydentach). Ważne jest, aby wnioski z monitoringu i incydentów realnie wpływały na zmianę podejścia do ryzyka, inwestycji oraz relacji z dostawcami.

Mapa obowiązków i praktyk: od regulacji do działań menedżerskich

Zastosowanie wymagań regulacyjnych i normatywnych wymaga przełożenia ich na praktykę i przypisania odpowiedzialności. W tabeli 1 zestawiono wybrane wymagania NIS2 i DORA oraz ich implikacje dla kadry zarządzającej.

Tabela 1. Wymogi *governance* w NIS2 i DORA oraz implikacje dla praktyk zarządczych

Źródło (regulacja/ standard)	Wymóg (skrót)	Implikacja dla kadry zarządzającej
NIS2 (art. 20)	Zatwierdzenie i nadzór; możliwa odpowiedzialność	Formalna decyzja organu zarządzającego: zatwierdzenie strategii cyber, polityk i planu wdrożenia; okresowy przegląd postępów.
NIS2 (art. 20)	Obowiązek szkoleń dla członków organu zarządzającego	Zaprojektowanie cyklu szkoleń dla zarządu/ rady (ryzyko, scenariusze, obowiązki, metryki); dokumentowanie udziału; regularność adekwatna do profilu ryzyka.
NIS2 (art. 21)	Minimalne kategorie środków (incydenty, BCP, łańcuch dostaw, ocena skuteczności, szkolenia, MFA)	Zapewnienie, że program bezpieczeństwa obejmuje obszary wymagane regulacyjnie; priorytetyzacja inwestycji.
DORA	Organ zarządzający definiuje, zatwierdza i odpowiada za ramy zarządzania ryzykiem ICT	Ustanowienie ram (*policy framework*), ról i odpowiedzialności; zapewnienie budżetu i zasobów; włączenie ryzyka ICT do decyzji strategicznych i operacyjnych.
DORA	Stałe podnoszenie kompetencji (regularne szkolenia)	Stały program rozwoju kompetencji cyfrowej odporności zarządu; ćwiczenia decyzyjne (*table-top*) i przeglądy po testach/ awariach.
NIST CSF 2.0 / ISO 27014	GOVERN/evaluate – direct – monitor – communicate	Zdefiniowanie apetytu na ryzyko, modelu raportowania KPI/KRI, mechanizmów eskalacji oraz przeglądów dojrzałości; powiązanie z celami biznesowymi i interesariuszami.

Źródło: opracowanie własne na podstawie: UE (2022a, 2022b); NIST (2024); ISO (2020).

Kluczowym wyzwaniem wdrożeniowym jest zdefiniowanie, „kto za co odpowiada", w sposób, który umożliwia sprawne podejmowanie decyzji i rozliczalność. W praktyce pomocna bywa macierz RACI, która rozróżnia odpowiedzialność wykonawczą (*responsible*) od odpowiedzialności właścicielskiej/rozliczalności (*accountable*). W tabeli 2 przedstawiono przykładową macierz dla wybranych obszarów.

Tabela 2. Przykładowa macierz RACI dla obszarów cyberbezpieczeństwa

Obszar decyzyjny	Rada/ Komitet	Zarząd/ CEO	CIO/ CTO	CISO	*Risk/ compliance*	Audyt wew.
Apetyt na ryzyko i priorytety	C	A	C	C	R	I
Strategia i polityki cyber	C/A*	A	C	R	C	I
Budżet i alokacja zasobów	C	A	R	C	C	I
Zarządzanie incydentami (decyzje kryzysowe)	I	A	R	R	C	C
Ciągłość działania/*disaster recovery*	I	A	R	C	R	C
Zarządzanie dostawcami ICT (ryzyko strony trzeciej) Raportowanie KPI/KRI i przeglądy dojrzałości	C	A	C	R	R	C

Legenda: R – responsible, A – accountable, C – consulted, I – informed.
Uwagi: C/A* – w zależności od modelu *corporate governance* rada nadzorcza może pełnić rolę A dla nadzoru, pozostawiając A operacyjne po stronie zarządu.

Źródło: opracowanie własne.

Kompetencje kadry zarządzającej i rola edukacji oraz HR

Przesunięcie cyberbezpieczeństwa do sfery odpowiedzialności kadry zarządzającej rodzi pytanie o wymagany profil kompetencji. NIS2 i DORA nie wymagają, aby członkowie zarządów byli ekspertami technicznymi; wymagają jednak wystarczającej wiedzy do identyfikacji ryzyk, oceny praktyk zarządzania ryzykiem oraz rozumienia wpływu cyberryzyka na usługi i operacje (UE, 2022a; UE, 2022b). Jednocześnie rośnie znaczenie struktur wspierających: komitetów ds. ryzyka i audytu, niezależnej funkcji CISO, mechanizmów trzeciej linii obrony (audyt), a także zewnętrznych benchmarków dojrzałości. Z perspektywy rozwoju zawodowego szczególnie istotne są trzy rodzaje kompetencji menedżerskich:

1) **nadzór korporacyjny i zarządzanie ryzykiem:** rozumienie apetytu na ryzyko, zasad ERM, odpowiedzialności prawnej, roli kontroli wewnętrznej oraz mechanizmów raportowania;

2) **podejmowanie decyzji inwestycyjnych w obszarze cyber:** (*trade-off* między bezpieczeństwem a zwinnością), priorytetyzacja portfela inicjatyw, zarządzanie długiem technologicznym;
3) **kompetencje przywódcze i kulturowe:** kształtowanie kultury cyberbezpieczeństwa, w której normy zachowań i procesy biznesowe sprzyjają ograniczaniu ryzyka (przykładowo: higiena cyfrowa, raportowanie incydentów, odpowiedzialność właścicieli procesów).

Zadaniem zespołów HR staje się przełożenie wymogów i oczekiwań na procesy: *onboarding* członków zarządu i kadry kierowniczej, plan szkoleń cyklicznych, system oceny kompetencji oraz mechanizmy motywacyjne. W kształceniu przyszłych menedżerów kluczowe jest, aby bezpieczeństwo cyfrowe stało się częścią programów z zakresu audytu, controllingu czy strategii, zamiast być ograniczanym wyłącznie do przedmiotów informatycznych. Praktyką o wysokiej wartości dydaktycznej są ćwiczenia typu *table-top* (symulacje decyzyjne), które pozwalają zarządom testować proces eskalacji, komunikacji i podejmowania decyzji w scenariuszach *ransomware* lub przerwania usług krytycznych.

Rekomendacje wdrożeniowe dla kadry zarządzającej

Na podstawie przedstawionych analiz można sformułować zestaw rekomendacji, które wspierają realizację odpowiedzialności zarządczej w cyberbezpieczeństwie:

1) **Ustanowienie jednoznacznej struktury odpowiedzialności:** formalnie umocować rolę CISO (lub równoważną) oraz określić relacje z CIO/CTO, ryzykiem, compliance i audytem.
2) **Zdefiniowanie tzw. apetytu na ryzyko cybernetyczne:** powiązanego z celami biznesowymi; przełożyć go na mierzalne KRI/KPI oraz progi eskalacji.
3) **Zatwierdzenie wieloletniego planu rozwoju dojrzałości cyfrowej** (*cyber maturity roadmap*), w której inicjatywy są priorytetyzowane na podstawie ryzyka i wartości biznesowej.
4) **Integracja wymogów cyberbezpieczeństwa z procesami zarządzania projektami i zmianą:** ocena ryzyka i wymagania bezpieczeństwa powinny być integralną częścią cyklu życia produktów i projektów (*security by design*).
5) **Zarządzanie ryzykiem strony trzeciej:** zdefiniowanie minimalnych wymagań wobec dostawców, prawo do audytu/raportów, mechanizmy monitoringu, a także scenariusze wyjścia.
6) **Testowanie odporności: regularne ćwiczenia scenariuszy** (*ransomware*, utrata danych, awaria dostawcy chmurowego), w tym elementy decyzyjne (kto podej-

muje decyzję o wyłączeniu systemu, komunikacji z klientami, współpracy z organami ścigania).

7) **Instytucjonalizowanie raportowania do zarządu i rady:** krótkie, porównywalne w czasie dashboardy, obejmujące zarówno ekspozycję na ryzyko, jak i skuteczność kontroli.
8) **Zbudowanie programów szkoleń i kompetencji:** dla organów zarządzających i kluczowej kadry, zgodny z wymaganiami NIS2/DORA, dokumentowane i regularnie aktualizowane.

Rekomendacje te wspierają przejście od podejścia „punktowej zgodności" (*compliance as a project*) do podejścia „odporności w działaniu" (*resilience as a capability*).

Podsumowanie

Cyberbezpieczeństwo konstytuuje się jako domena odpowiedzialności kadry zarządzającej nie tylko w wymiarze technologicznym, lecz przede wszystkim w aspekcie implikacji biznesowych oraz formalnoprawnych uwarunkowań tejże odpowiedzialności. NIS2 i DORA wprost formułują obowiązki zatwierdzania, nadzorowania i rozwijania kompetencji przez organy zarządzające, co przesuwa cyberryzyko do „rdzenia" *corporate governance* (UE, 2022a; UE, 2022b). Proponowany model cyklu odpowiedzialności zarządczej oraz mapy ról (RACI) stanowią narzędzia, które mogą wspierać zarówno praktykę zarządzania, jak i edukację menedżerów.

Ograniczeniem artykułu jest jego koncepcyjno-przeglądowy charakter oraz koncentracja na wybranych regulacjach i standardach. Dalsze badania mogłyby obejmować empiryczną ocenę dojrzałości *governance cyber* w organizacjach w Polsce, analizę wpływu kompetencji zarządów na wyniki bezpieczeństwa oraz identyfikację najlepszych praktyk dydaktycznych w kształceniu menedżerów w obszarze cyberodporności.

Bibliografia

ENISA (2025). *ENISA Threat Landscape 2025*, European Union Agency for Cybersecurity. Pobrano z: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025 (dostęp: 10.01.2026).

Harel, Y. (2025). Strategic Cybersecurity Oversight Framework: A Board's Imperative. *Cybersecurity*, 11(1), tyaf021.

IBM Security (2024). *Cost of a Data Breach Report 2024*. Pobrano z: https://cdn.table.media/assets/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf (dostęp: 10.01.2026).

ISO (2018). ISO 31000:2018 – Risk Management – Guidelines: Geneva: International Organization for Standardization, https://www.iso.org/standard/65694.html.

ISO (2020). ISO/IEC 27014:2020 – Governance of Information Security. Geneva: International Organization for Standardization, https://www.iso.org/standard/74046.html.

ISO (2022). ISO/IEC 27001 – Information Security Management Systems (updated 2022). Geneva: International Organization for Standardization, https://www.iso.org/standard/27001.

Lowry, M.R., Offenberg, D., Wang, X. (2025). Inexpert Supervision: Field Evidence on Boards' Oversight of Cybersecurity Risk. *Management Science*, 72(2), 783–804. Pobrano z: https://pubsonline.informs.org/doi/10.1287/mnsc.2023.04147 (dostęp: 10.01.2026).

Ministerstwo Cyfryzacji (2025). *Nowe przepisy wzmocnią ochronę przed cyberzagrożeniami*. Pobrano z: https://www.gov.pl/web/cyfryzacja/nowe-przepisy-wzmocnia-ochrone-przed-cyberzagrozeniami (dostęp: 10.01.2026).

NIST (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. National Institute of Standards and Technology, Gaithersburg, MD, NIST Cybersecurity White Paper 29. DOI: 10.6028/NIST.CSWP.29.

Posthumus, S., Solms, R. von (2004). A Framework for the Governance of Information Security. *Computers & Security*, 23(8), 638–646. DOI: 10.1016/j.cose.2004.10.006.

Solms, R. von, Solms, S.H. von (2006). Information Security Governance: A Model Based on the Direct – Control Cycle. *Computers & Security*, 25(6), 408–412. DOI: 10.1016/j.cose.2006.07.005.

UE (2022a). Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. (NIS2), Bruksela, Dziennik Urzędowy UE, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A02022L2555-20221227.

UE (2022b). Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2554 z dnia 14 grudnia 2022 r. (DORA), Bruksela, Dziennik Urzędowy UE, https://eur-lex.europa.eu/legal-content/EN-CS/TXT/?uri=CELEX%3A32022R2554.

Cybersecurity as an Area of Management Responsibility: From Regulatory Compliance to Building Organizational Resilience

Abstract

The increasing scale and complexity of digital threats make cybersecurity a core management responsibility rather than an IT-only domain. Recent EU regulations reinforce this shift: the NIS2 Directive requires management bodies to approve and oversee cybersecurity risk-management measures and enables liability for non-compliance, while the DORA Regulation stresses the management body's full and ultimate responsibility for ICT risk management in the financial sector, alongside continuous training. This paper integrates

regulatory and normative requirements (NIS2, DORA, NIST CSF 2.0, ISO/IEC 27001 and ISO/IEC 27014) with academic research on information security governance. It proposes a 'managerial accountability cycle' and a set of implementation practices covering risk appetite definition, resource allocation, ICT supply-chain oversight and cybersecurity culture. Implications for management education and HR development are discussed.

Keywords: cybersecurity, managerial accountability, governance, risk management, NIS2, DORA

Izabela Markiewicz

Absolwentka studiów I stopnia na kierunku bezpieczeństwo wewnętrzne (Wydział Nauk Politycznych i Studiów Międzynarodowych, Uniwersytet Warszawski, Polska). Obecnie studentka studiów II st. na kierunku cyberbezpieczeństwo (Wydział Nauk Politycznych i Studiów Międzynarodowych, Uniwersytet Warszawski, Polska).
i.markiewic2@student.uw.edu.pl
ORCID: 0009-0006-4697-2296