CyberMSME

Cyberbezpieczeństwo dla mikro, małych i średnich firm

Radzenie sobie z niepewnością, niejednoznacznością i ryzykiem w środowisku cybernetycznym

Autor: IDP European Consultants

Erasmus+

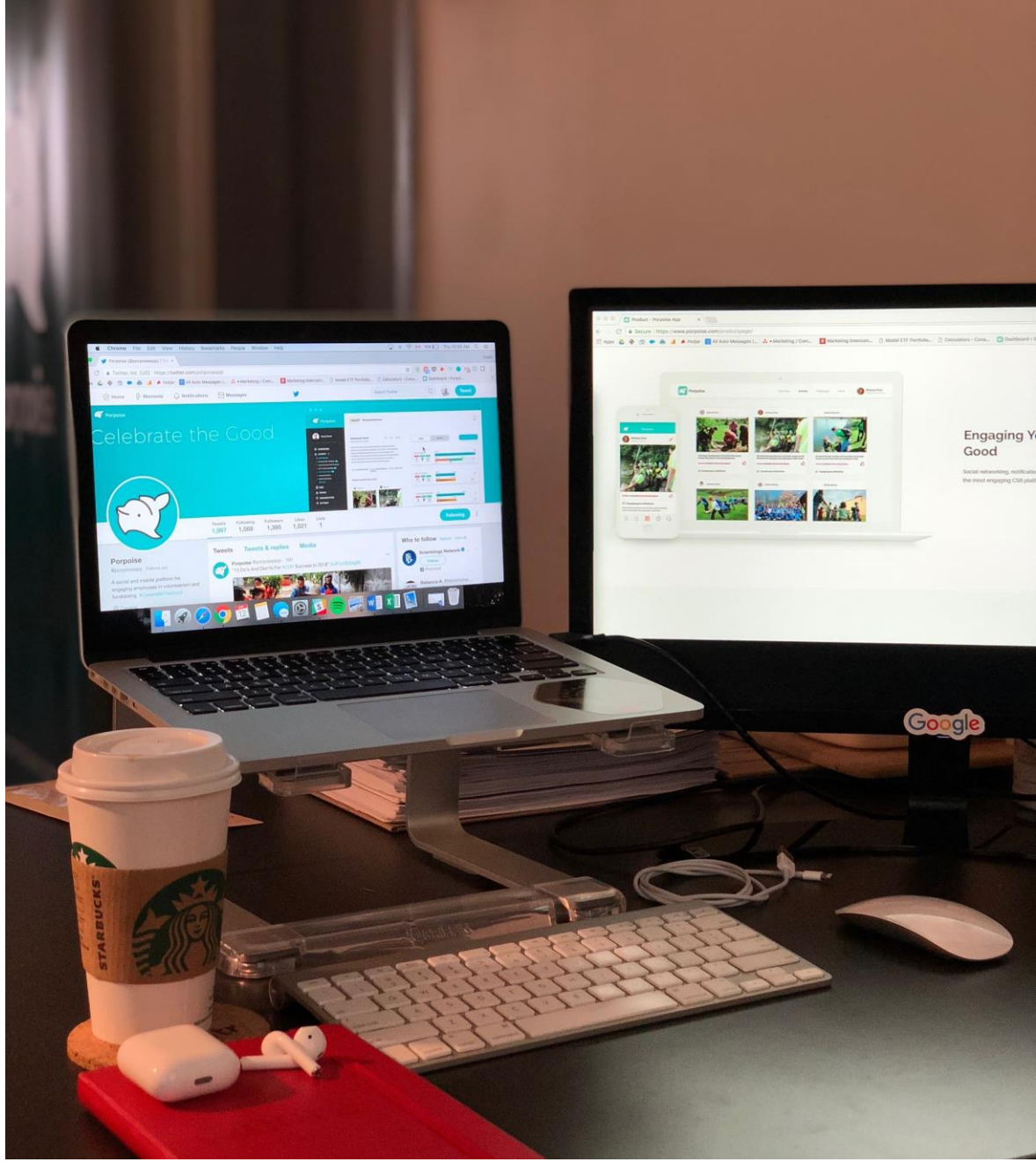
Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Cele i założenia:

Celem tego modułu jest wykształcenie w czytelnikach odnowionej świadomości na temat strategicznej roli zarządzania ryzykiem (cybernetycznym) dla mikro- i małych przedsiębiorstw działających w ramach połączonego ekosystemu cyfrowego.

Zawartość tego modułu ma na celu pomoc w zdobyciu nowej agendy dla zarządzania ryzykiem jako funkcji biznesowej, która przenika wszystkie zadania i działania, odpowiadając na nową pilną potrzebę ochrony firm przed zagrożeniami cybernetycznymi.

Zrobimy to poprzez dzielenie się godnymi zaufania, solidnymi i wiarygodnymi ramami zarządzania, które mają tradycyjne zastosowanie we wszystkich funkcjach biznesowych.



Erasmus+

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Indeks

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Rozdział 1: Sposób zarządzania ryzykiem cybernetycznym dla MMŚP

1.1: Uwagi wstępne

Zawartość tego modułu szkoleniowego stanowi *nieoficjalną* kontynuację programu **EntreComp w zakresie gotowości do podejmowania ryzyka cybernetycznego.**

W poprzednim module odnieśliśmy się do kilku ram, które pomagają lepiej przygotować się do oceny i oszacowania ryzyk i zagrożeń cybernetycznych w środowisku IT.

W tym module przedstawimy Ci koncepcyjne mapy ułatwiające poruszanie się w obszarze bezpieczeństwa cybernetycznego, gotowości oraz odporności cybernetycznej z perspektywy zapewnienia jakości i zarządzania ryzykiem.

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Rozdział 1: Sposób zarządzania ryzykiem cybernetycznym dla MMŚP

1.1: Uwagi wstępne

Obecnie, gdy zagrożenie cybernetyczne dotyka firmy i organizacje coraz bardziej, bezpieczeństwo cybernetyczne staje się głównym przedmiotem zainteresowania nie tylko specjalistów IT, ale także specjalistów i ekspertów działających w dziedzinie zarządzania ryzykiem. Organizacje w coraz większym stopniu polegają na narzędziach cyfrowych w celu planowania, zarządzania i rozwijania swojej działalności, a wszelkie zakłócenia w stworzonym w ten sposob "cyfrowym łańcuchu wartości" przekładają się na poważne konsekwencje, na które nierzadko organizacje nie są przygotowane.

Być może słyszałeś/-aś popularne, ale błędne przekonanie na temat cyberbezpieczeństwa, wedle którego zabezpieczanie systemów informatycznych przed cyberzagrożeniami wymaga skomplikowanych i wysoce wyrafinowanych procedur informatycznych. Choć z pewnością prawdą jest, że specjaliści od cyberbezpieczeństwa dysponują zaawansowaną wiedzą inżynierską i know-how, określony sposób myślenia jest w zasięgu każdego...

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Rozdział 1: Sposób zarządzania ryzykiem cybernetycznym dla MMŚP

1.1: Uwagi wstępne

Kluczowe wnioski z raportu IBM z 2021 roku wskazują, że cyberodporność to kilka prostych działań:

- inwestowanie w prewencję (tj. identyfikację i ocenę ryzyka)
- moduł bezpieczeństwa Zero-Trust (zastanów się, kto ma dostęp do Twoich danych)
- testy warunków skrajnych (pomiar i ocena wewnętrznych strategii odporności)
- zarządzanie tożsamością i dostępem w celu zarządzania pracownikami zdalnymi (jeszcze ważniejsze niż w erze inteligentnej pracy)
- programy zgodności: pielęgnowanie cyberkultury na poziomie międzyfunkcjonalnym
- zmniejszanie złożoności (wyrafinowana prostota)
- zmniejszanie luki w umiejętnościach

Erasmus+

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Rozdział 1: Sposób zarządzania ryzykiem cybernetycznym dla MMŚP

1.1: Uwagi wstępne

W rzeczywistości, dowody z wyżej wymienionego raportu wskazują, że główne czynniki zakłócające są związane z działalnością ludzką, a nie z niewydolnością technologiczną:

Siatki bezpieczeństwa		Dystratory
Testy Red Team	Grupa zadaniowa ds. zarządzania ryzykiem	Braki w zgodności
Platforma AI	Zapobieganie utracie danych	Migracja w chmurze
Zaangażowanie zarządu	Szerokie szyfrowanie	Narażenie IoT / OT
Doświadczony CISO	Utworzenie zespołu PR	Zgubione lub skradzione urządzenia
Procedury ograniczania ryzyka	Cyberbezpieczeństwo	Pracownicy zdalni
DevSecOps	Zarządzane usługi bezpieczeństwa	Niedobór umiejętności w zakresie bezpieczeństwa
Wymiana informacji o zagrożeniach	Badanie podatności na zagrożenia	Złożone procesy wewnętrzne
Szkolenie pracowników	Ochrona przed kradzieżą tożsamości	Naruszenie przepisów przez osoby trzecie
Analityka bezpieczeństwa		

Źródło: IBM, 2021 r.

Erasmus+

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Rozdział 1: Sposób zarządzania ryzykiem cybernetycznym dla MMŚP

1.2: Zarządzanie ryzykiem

Dowody zebrane przez partnerów Cyber MMŚP wskazują, że brak niezawodnego systemu zarządzania (cyber)ryzykiem jest jedną z najczęstszych przyczyn narażenia na ryzyko cybernetyczne.

Wynik ten świadczy, że o cyberbezpieczeństwa nie jest uznawane za jeden z najważniejszych problemów w zakresie odporności i konkurencyjności przedsiębiorstw.

→ Zarządzanie ryzykiem cybernetycznym powinno opierać się na tych samych paradygmatach i koncentrować się na tych samych działaniach (tj. monitorowaniu i ocenie), co każda inna podstawowa funkcja. To z kolei będzie dowodzić przewagi konkurencyjnej, jaką dysponuje dana firma, w obliczu potrzeby adaptaci i rekacji na nowe, wciąż rozwijające się zagrożenia mające swoje źródło w zmianach rynkowych lub społecznych.

Erasmus+

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Rozdział 1: Sposób zarządzania ryzykiem cybernetycznym dla MMŚP

1.2: Zarządzanie ryzykiem, ISO 31000

Międzynarodowa Organizacja Normalizacyjna uznaje zarządzanie ryzykiem za proces obejmujący **systematyczne stosowanie** polityk, procedur i praktyk w zakresie działań komunikacyjnych
i konsultacyjnych, ustalania kontekstu oraz oceny, leczenia, monitorowania, przeglądu, rejestrowania i raportowania ryzyka.

Ponieważ wszystkie funkcje biznesowe pozostają związane z wydajnością oraz efektywnością systemów i sieci IT regulujących przepływ ich zadań, zarządzanie ryzykiem cybernetycznym staje się integralną częścią strategicznego podejmowania decyzji i planowania długoterminowego.

Zarządzanie ryzykiem cybernetycznym jest procesem cyklicznym i obejmuje bieżące mechanizmy ukierunkowane na osiąganie coraz wyższych standardów.

Kontrola > **Ocena** > **Dopracowanie**

Erasmus+

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Rozdział 1: Sposób zarządzania ryzykiem cybernetycznym dla MMŚP

1.2: ISO 31000, wizualna reprezentacja

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Rozdział 1: Sposób zarządzania ryzykiem cybernetycznym dla MMŚP

1.3: Ograniczanie ryzyka cybernetycznego

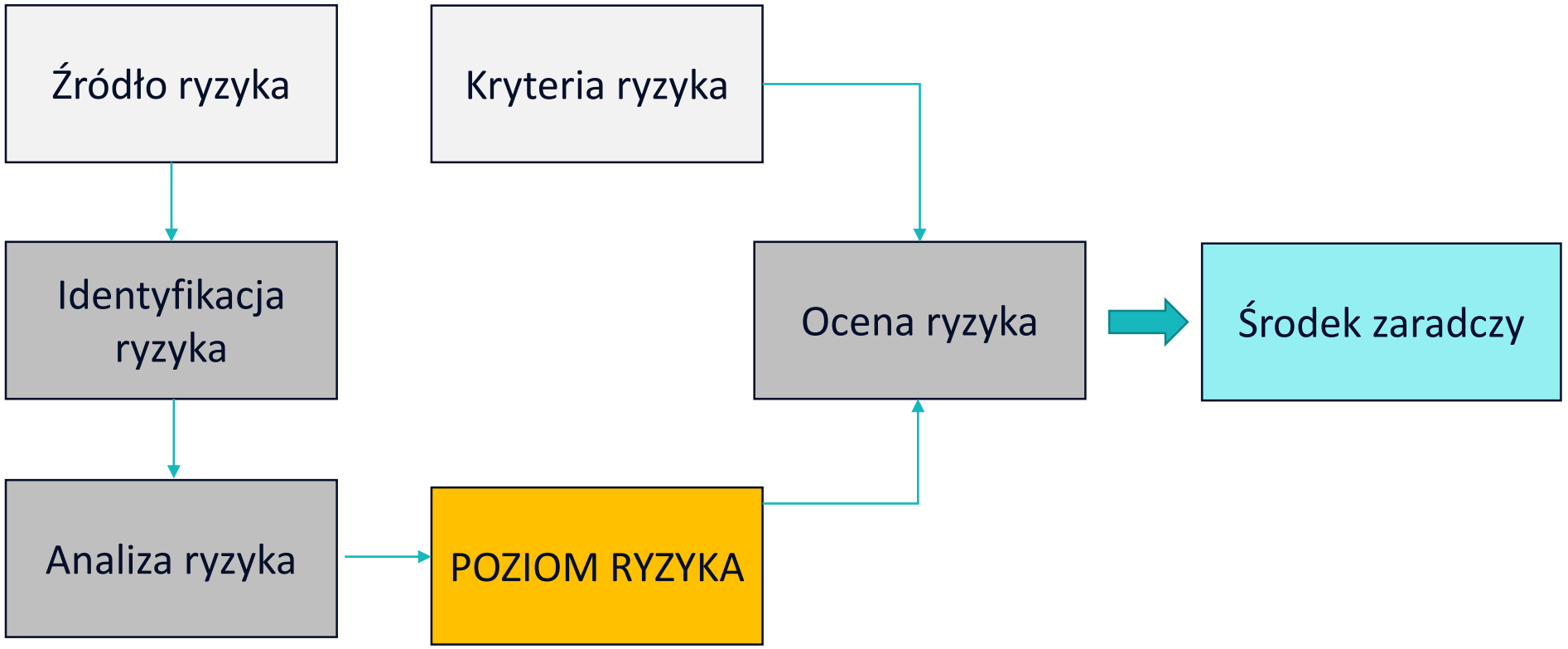
Zgodnie z normą ISO 31000, modele zarządzania cyberryzykiem wewnętrznym powinny odzwierciedlać wartości, cele i zasoby organizacji oraz być zgodne z polityką i deklaracjami dotyczącymi zobowiązań organizacji oraz poglądami interesariuszy.

Gdy organizacja ustali zakres, kontekst i kryteria modelu zarządzania, zaleca się przystąpienie do właściwej oceny.Ocena kończy się trzyetapowym procesem:

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Rozdział 1: Sposób zarządzania ryzykiem cybernetycznym dla MMŚP

1.4: Przepływ oceny ryzyka



Źródło: Caliste, J.-P & Heitor, Jone (2020)

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Rozdział 1: Sposób zarządzania ryzykiem cybernetycznym dla MMŚP

1.5: Siatka oceny ryzyka

skutki (lub kryteria ryzyka)

prawdopodobieństwo	Nieistotne	Marginalne	Krytyczne	Katastrofalne
Spore				
Prawdopodobne				
Ewentualne				
Nieprawdopodobne				
Małe				

NASA, Goddard Space Flight Center, Goddard Technical Standard GSFC-STD-0002, Risk Management Reporting

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Rozdział 2: Zapewnienie jakości w zakresie cyberhigieny

2.1: Wprowadzenie do Zapewnienia Jakości

Specjaliści i eksperci w dziedzinie zarządzania przedsiębiorstwem z pewnością słyszeli o Lean Manufacturing, Total Quality Management (TQM), Just In Time (JIT) itp.

Powyższe terminy odnoszą się do najlepiej rozpowszechnionych ram audytowych w procesie zarządzania jakością. Wdraża się je w przemyśle.

Wszystkie 3 modele mają jedną wspólną cechę: wywodzą się z Japonii, a na świecie stały się zyskały popularność jako punkty odniesienia dla procedur audytu i zapewniania jakości.

Erasmus+

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Rozdział 2: Zapewnienie jakości w zakresie cyberhigieny

2.2: Wprowadzenie do Zapewnienia Jakości — KAIZEN

To, co jest mniej znane na temat TQM i JIT, to "filozofia" biznesu, z której się wyłoniły: Kaizen (改善), dosłownie tłumaczona jako 改 = zmiana,善 = dobry.

Kultura Kaizen zakłada stałe i ciągłe ustanawianie wyższych standardów wydajności.

Około lat 80. stała się ona dominującym paradygmatem biznesowym w przemyśle japońskim, ze szczególnym uwzględnieniem Toyoty (tj. Toyota Production System, *Toyotism*).

Pomimo wszystkiego, co może się wydawać, kultura Kaizen nie jest jednak w pełni japońskim produktem.

Erasmus+

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

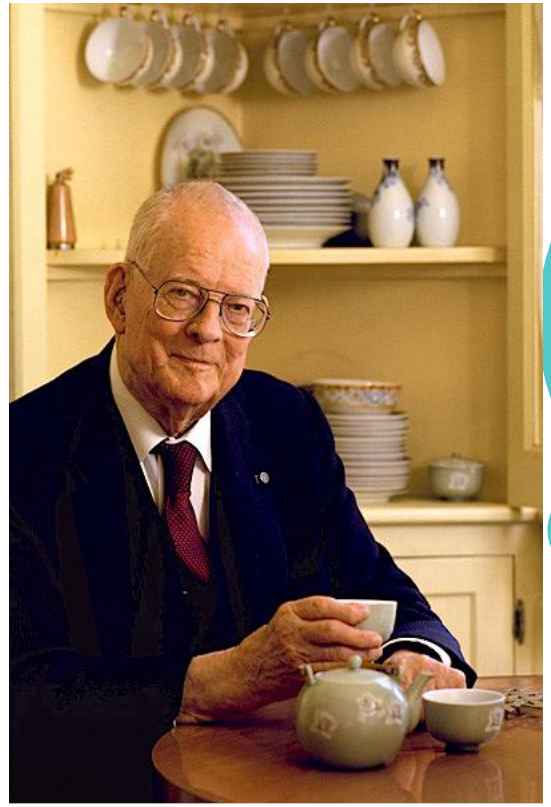
Rozdział 2: Zapewnienie jakości w zakresie cyberhigieny

2.3: Wprowadzenie do Zapewnienia Jakości — Deming

Model Kaizen wywodzi się z międzynarodowego programu współpracy przemysłowej pomiędzy USA a Japonią, rozpoczętego pod koniec II wojny światowej.

Dokładniej rzecz ujmując, początki obecnego modelu Kaizen zostały zainspirowane pracą amerykaskiego statystyka, W. Edwardsa Deminga (1990-1993).

W. Edwards Deming jest twórcą jednej z pierwszych ram referencyjnych dla zapewnienia jakości i audytu. Jest to tzw. model Deminga.

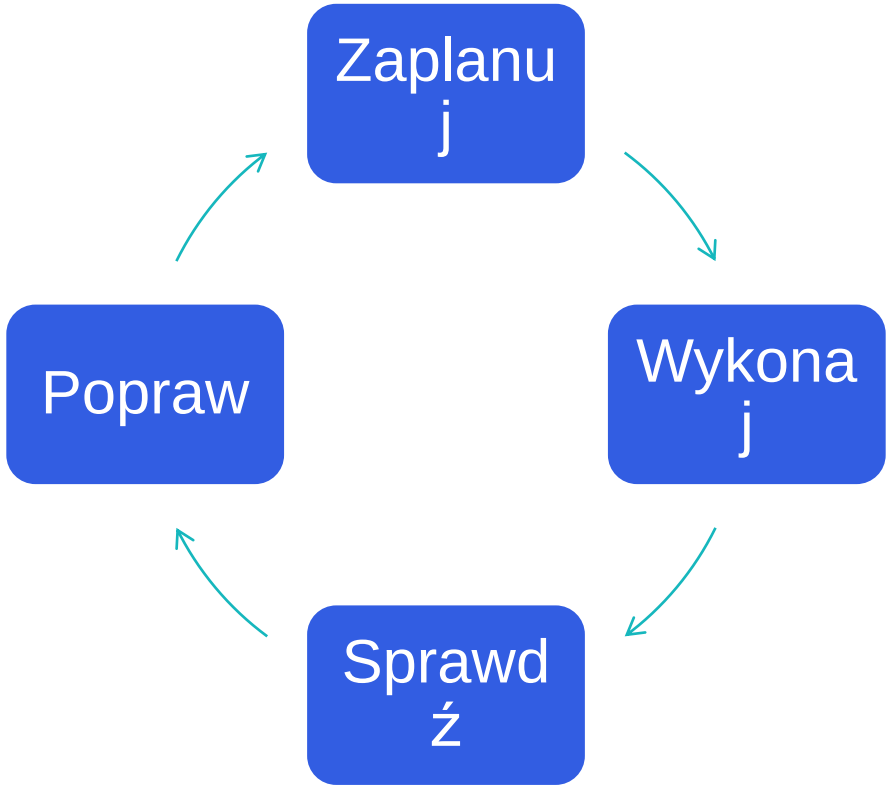


Erasmus+

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Rozdział 2: Zapewnienie jakości w zakresie cyberhigieny

2.3: Model Deminga



Źródło: Deming, W.E., 1950. Elementarne zasady statystycznej kontroli jakości, JUSE.

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Rozdział 2: Zapewnienie jakości w zakresie cyberhigieny

2.3: Wprowadzenie do Zapewnienia Jakości — Deming

Model Deminga doczekał się na przestrzeni lat różnych adaptacji propagowanych przez innych autorów. Kaizen jest oczywiście jedną z nich.

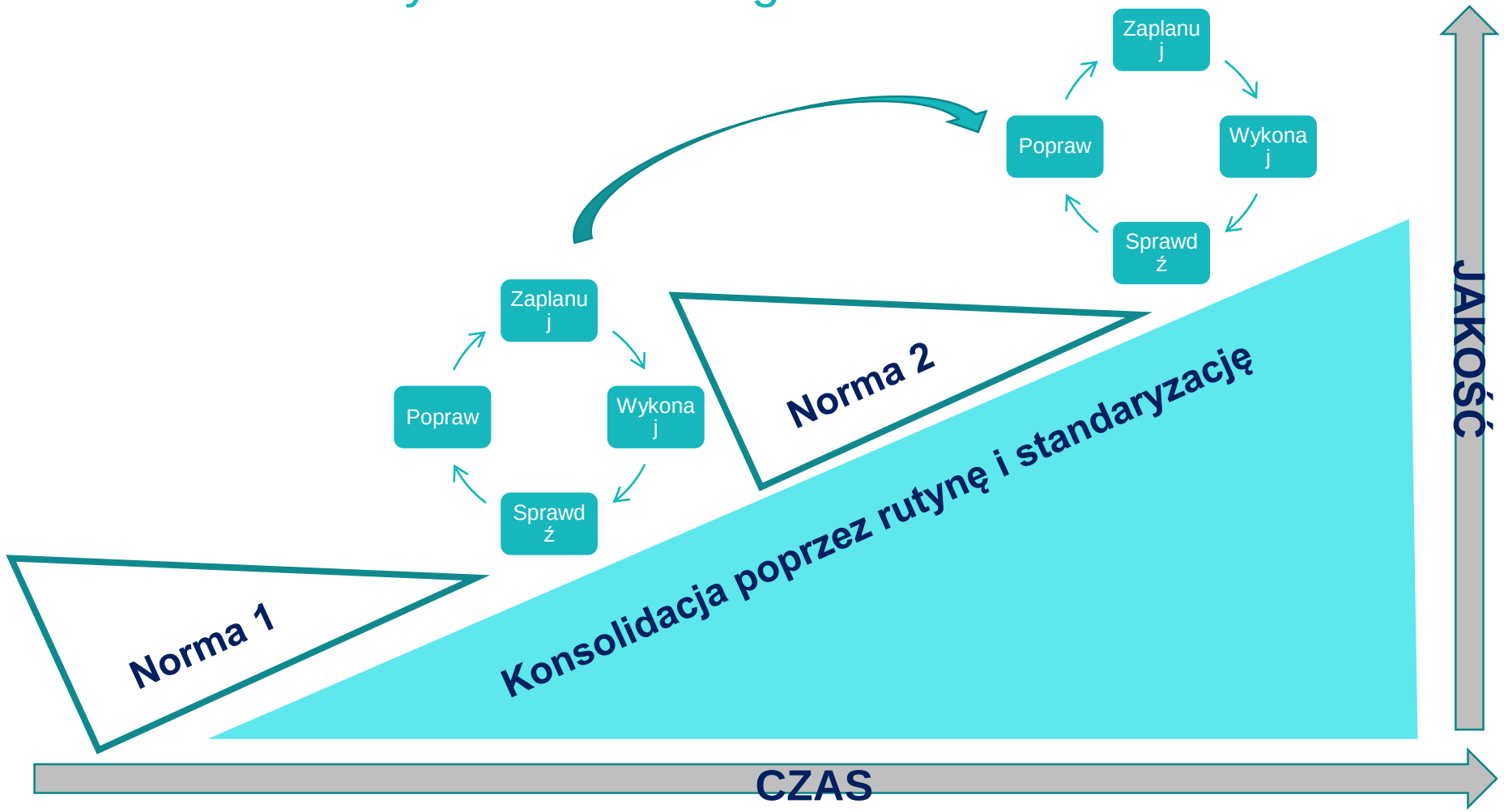
Do dziś *oryginalny* model Deminga stanowi inspirację dla normy ISO 9001 w zakresie zasad zarządzania jakością.

Spośród wszystkich readaptacji modelu Deminga chcielibyśmy Ci zaproponować tę przedstawioną w perspektywie ewolucyjnej. Znajdziesz ją na następnym slajdzie.

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Rozdział 2: Zapewnienie jakości w zakresie cyberhigieny

2.3: Zaawansowany model Deminga



Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Rozdział 2: Zapewnienie jakości w zakresie cyberhigieny

2.3: Model Deminga — uwagi

Największą zaletą modelu Deminga, która pozwoliła mu przejść próbę czasu, jest to, że:

- jest łatwy do zrozumienia
- może być stosowany przez każdą organizację — niezależnie od branży
- można go zastosować do każdego procesu i funkcji biznesowej — w tym do cyberbezpieczeństwa

Z normy ISO 31000 wynika, że kompleksowy model zarządzania ryzykiem uwzględnia przekrojowy i ciągły proces monitorowania i oceny.

Cykl DEMING obejmuje oba te priorytety, ponieważ pozwala użytkownikom na:

1. Opracowanie strategii najbardziej odpowiednich rozwiązań w zakresie bezpieczeństwa cybernetycznego z uwzględnieniem mapowanych ryzyk i warunków organizacyjnych
2. Wdrożenie wyżej wymienionych
3. Ocenę i zatwierdzenie ich adekwatności
4. Odpowiednią reakcję

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Rozdział 2: Zapewnienie jakości w zakresie cyberhigieny

2.4: Ocena kształtująca vs. ocena podsumowująca

Możesz podzielić procesu ewaluacji (tj. fazy sprawdzania) na dwie odrębne części, w zależności od rzeczywistego czasu na przeprowadzenie oceny:

Ocena kształtująca	Ocena podsumowująca
Ocena procesów krok po kroku i ocena działań dzień po dniu.	Po zakończeniu każdego większego zadania spójrz wstecz na to, co zostało zrobione i spróbuj porównać to z przewidywanymi standardami/ oczekiwaniami.

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Podsumowanie

Główne wnioski

- Przekształcenie zarządzania ryzykiem z funkcji horyzontalnej w kluczowe zasoby wewnętrzne zapewnia sukces konkurencyjny
- Zarządzanie ryzykiem to sposób myślenia, a nie podejście operacyjne
- Świadomość → gotowość → odporność
- Ograniczanie ryzyka i środki zaradcze: identyfikacja, analiza i ocena
- Ocena ryzyka: prawdopodobieństwo vs. wpływ
- Zapewnienie jakości: stałe i ciągłe doskonalenie

Erasmus+

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.

Dziękujemy

za uwagę!

Wsparcie Komisji Europejskiej dla powstania tej publikacji nie oznacza poparcia dla jej treści, które odzwierciedlają jedynie poglądy autorów, a Komisja nie ponosi odpowiedzialności za jakiekolwiek wykorzystanie informacji w niej zawartych.