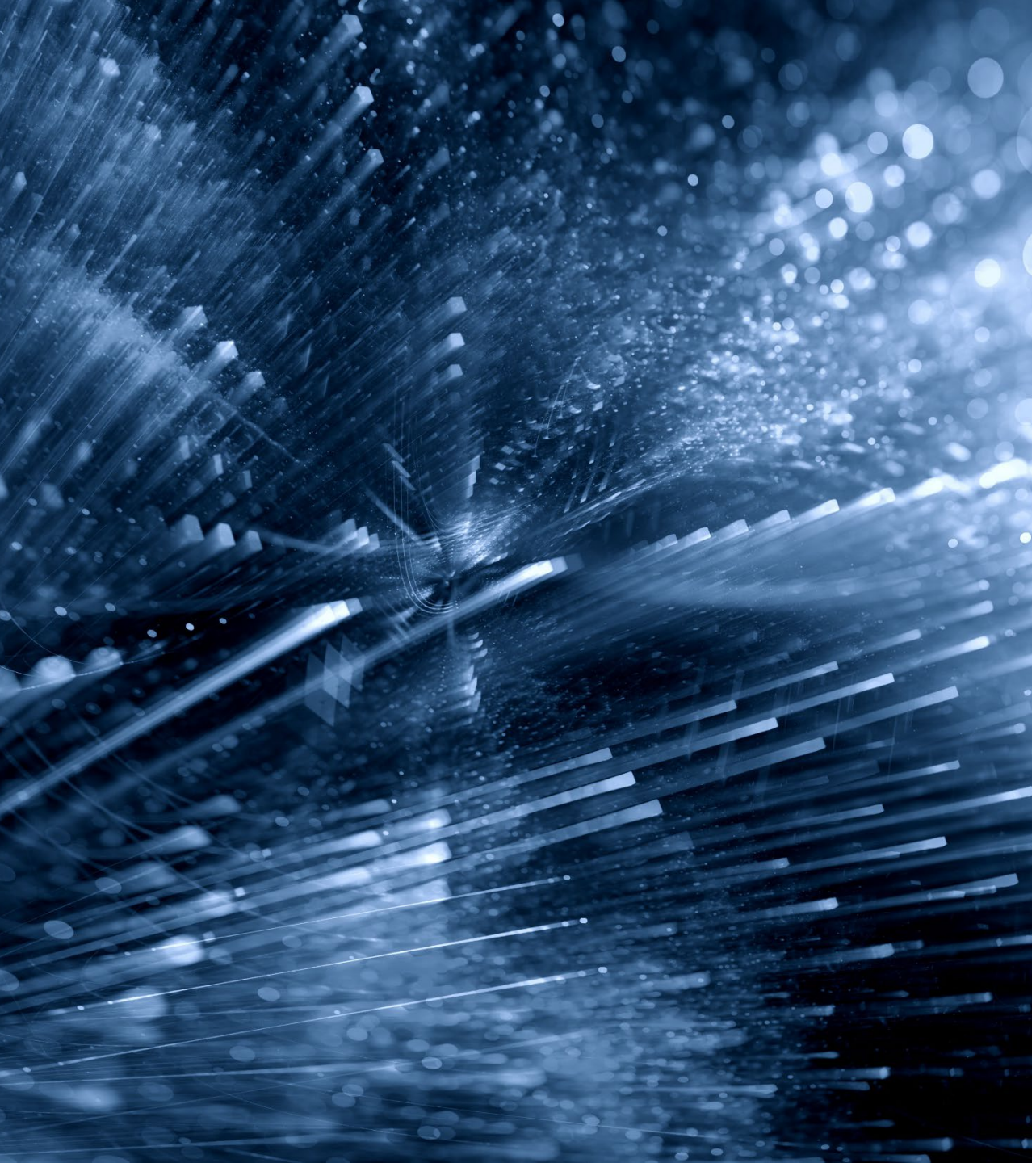


CYBERBEZPIECZEŃSTWO
RÓŻNE PERSPEKTYWY POSTRZEGANIA

dr inż. Jacek Oko
Prezes UKE

Urząd Komunikacji Elektronicznej | UKE

BEZPIECZEŃSTWO

Powszechnie rozumiane jako:
„stan dający poczucie pewności i gwarancję jego zachowania oraz szansę na doskonalenie”

W normalizacji przyjęto, że termin „bezpieczeństwo” oznacza :
„brak nieakceptowanego ryzyka szkód”

Mówimy o zarządzaniu ryzykiem jako procesem budowania bezpieczeństwa organizacji, regionu, państwa.

BEZPIECZEŃSTWO W ASPEKCIE 5G

Sieć 5G jest pierwszą w historii komunikacji mobilnej, która została zaprojektowana z myślą o maszynach.

Zgodnie z zapowiedziami, technologia 5G ma stać się kręgosłupem współczesnej gospodarki, ale również infrastruktury krytycznej, od której zależy bezpieczeństwo kraju.

Z punktu widzenia technologicznego, budowa sieci 5G wymaga absolutnie holistycznego podejścia do spraw bezpieczeństwa, a nie skupiania się na pojedynczych elementach technicznych.

Sposób w jaki wszystkie technologie związane z 5G są budowane, zintegrowane, czy kontrolowane, jest podstawą zarządzania zaufaniem.

BEZPIECZEŃSTWO W ASPEKCIE 5G

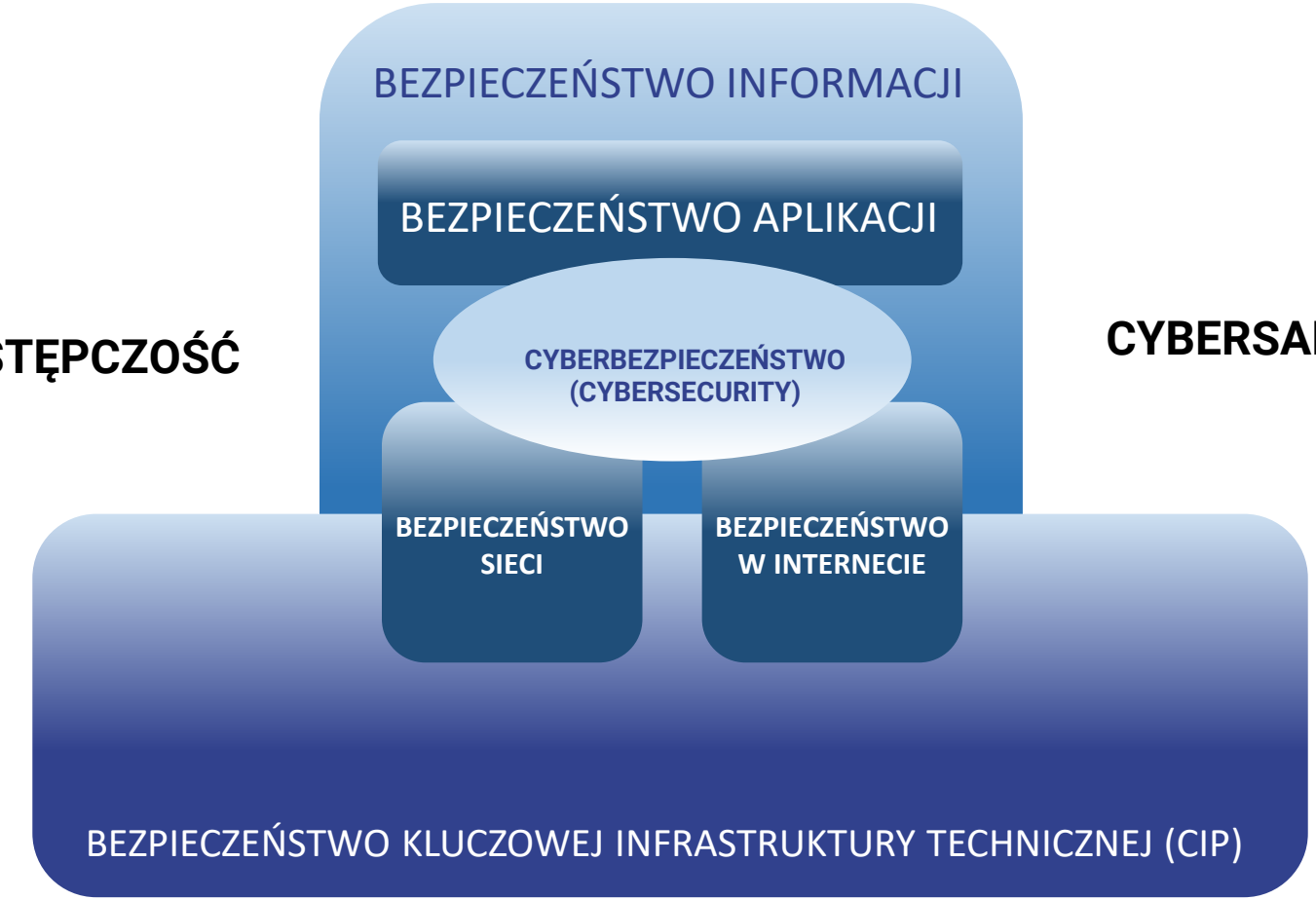
Nie ma jednego, powszechnie akceptowanego modelu organizacyjnego bezpieczeństwa - jest zbyt wiele czynników, które mają wpływ na zaprojektowanie optymalnego rozwiązania .

Sytuację pogarsza utrzymujący się niedobór umiejętności w zakresie bezpieczeństwa, który sprawia, że organizacje / przedsiębiorstwa są bardziej zależne od zasobów zewnętrznych (np. konsultantów, wykonawców i dostawców usług zarządzanych), co znowu stawia nowe wymagania w zakresie zarządzania działaniami (w tym ryzykiem).

Liderzy ds. Bezpieczeństwa i zarządzania ryzykiem w organizacjach muszą wziąć pod uwagę szeroki zakres czynników i sprawdzonych praktyk podczas projektowania swoich organizacji bezpieczeństwa, w tym między innymi dojrzałość, ład korporacyjny, wielkość, kulturę i budżet.

MODELOWE SPOJRZENIE NA CYBERBEZPIECZEŃSTWO

CYBERPRZESTĘPCZOŚĆ



CYBERSAFETY

BEZPIECZEŃSTWO W ASPEKCIE 5G

Różnorodność postrzegania, czy „tylko” perspektywy spojrzenia?

- Ujęcie organizacji bezpieczeństwa rozwiązań (w tym ujęcie sieci 5G)
- Grupy Państw (organizacja ponadregionalna) - ENISA
- Państwowego – CISA
- Analityka rynku – na przykładzie Gartner / zarządzanie ryzykiem
- Producenta rozwiązań - na przykładzie Ericsson

STRATEGIA ENISA / UE

Strategia proponuje konkretne cele dla Agencji w postaci siedmiu celów strategicznych, które określą priorytety Agencji Unii Europejskiej ds. Cyberbezpieczeństwa na najbliższe lata.

Te cele strategiczne są następujące:

- Umocnione i zaangażowane społeczności w całym ekosystemie cyberbezpieczeństwa;
- Cyberbezpieczeństwo jako integralna część polityk UE;
- Skuteczna współpraca między podmiotami operacyjnymi w Unii w przypadku masowych incydentów cybernetycznych;
- Przełomowe kompetencje i zdolności w zakresie cyberbezpieczeństwa w całej Unii;
- Wysoki poziom zaufania do bezpiecznych rozwiązań cyfrowych;
- Prognozowanie pojawiających się i przyszłych wyzwań w zakresie bezpieczeństwa cybernetycznego;
- Wydajne i skuteczne zarządzanie informacjami i wiedzą w zakresie cyberbezpieczeństwa w Europie.

STRATEGIA CISA / USA

W sierpniu 2020 r. Agencja Cyberbezpieczeństwa i Bezpieczeństwa Infrastruktury (CISA) opublikowała swoją strategię zapewnienia bezpieczeństwa i odporności infrastruktury 5G w Stanach Zjednoczonych .

Cel strategii:

- Biorąc pod uwagę zarówno potencjał, jak i ryzyko i wyzwania związane z technologią 5G, zwłaszcza w krytycznych infrastrukturach i usługach, CISA opracowała strategię 5G.

- Celem strategii 5G CISA jest przyspieszenie rozwoju i wdrożenia bezpiecznej i odpornej infrastruktury 5G, która promuje bezpieczeństwo narodowe, integralność danych, innowacje technologiczne i możliwości gospodarcze dla Stanów Zjednoczonych i ich sojuszniczych partnerów.

STRATEGIA CISA / USA

Wizja CISA skupia się na połączeniu handlu, bezpieczeństwa i relacji globalnych i wymienia trzy podstawowe kompetencje jako podstawę jej podejścia:

- Zarządzanie ryzykiem w celu promowania bezpiecznego i odpornego wdrożenia 5G poprzez identyfikację, analizę, ustalanie priorytetów i zarządzanie ryzykiem
- Zaangażowanie interesariuszy poprzez aktywne angażowanie federalnych, stanowych, lokalnych, plemiennych i terytorialnych, branżowych, akademickich i międzynarodowych partnerów w rozwiązywaniu problemów związanych z 5G
- Pomoc techniczna w zakresie aktualizacji i opracowywania narzędzi i usług, które wspierają zainteresowane strony w planowaniu, zarządzaniu, operacyjnymi i technicznymi aspektami bezpiecznego wdrażania 5G

IMPLEMENTACJA 5G – ZAGROŻENIA/BEZPIECZEŃSTWO

Odpowiedzialne podejście Producenta rozwiązań w sferze sieci i urządzeń

Przykład: Ericsson / Trust stack

Filozofia cyberbezpieczeństwa sieci 5G opiera się na czterech podstawowych aspektach, określanych jako stos zaufania (trust stack).

Stos zaufania uwzględnia wszystkie elementy powstawania sieci:

- proces standaryzacji (normalizacja)
- produkcja elementów oraz oprogramowania
- budowa sieci
- eksploatacja

IMPLEMENTACJA 5G – ZAGROŻENIA/BEZPIECZEŃSTWO

Odpowiedzialne podejście Producenta rozwiązań w sferze sieci i urządzeń

Przykład: Ericsson / Trust stack

Filozofia cyberbezpieczeństwa sieci 5G opiera się na czterech podstawowych aspektach, określanych jako stos zaufania (trust stack).

Stos zaufania uwzględnia wszystkie elementy powstawania sieci:

1) **proces standaryzacji**
2) **produkcja elementów oraz oprogramowania**
3) **budowa sieci**
4) **eksploatacja**

IMPLEMENTACJA 5G – ZAGROŻENIA/BEZPIECZEŃSTWO

Odpowiedzialne podejście Producenta rozwiązań w sferze sieci i urządzeń

Przykład: Ericsson / Trust stack

Filozofia cyberbezpieczeństwa sieci 5G opiera się na czterech podstawowych [illegible] określanych jako stos zaufania (trust stack).

Stos zaufania uwzględnia wszystkie [illegible] sieci:

1) **proces standaryzacji**
2) **produkcja elementów oraz oprogramowania**
3) **budowa sieci**
4) **eksploatacja**

UWAGA:

Skuteczność bezpieczeństwa sieci 5G jest zależna od wszystkich powyższych elementów.

IMPLEMENTACJA 5G – ZAGROŻENIA/BEZPIECZEŃSTWO

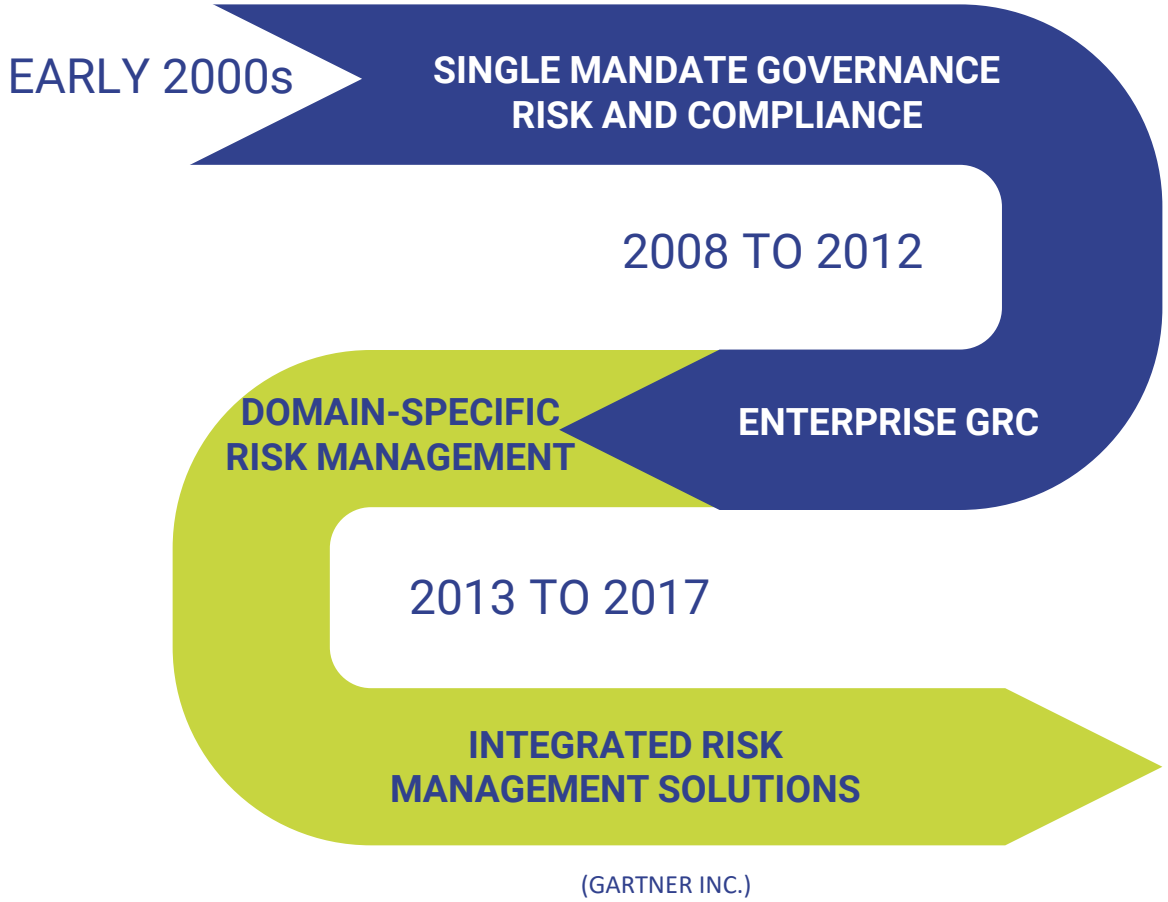
Odpowiedzialne podejście Producenta rozwiązań w sferze sieci i urządzeń

Przykład: Ericsson / Trust stack

Rozwinięciem stosu zaufania jest spojrzenie na proces wdrażania sieci klasy 5G:

1) Normalizacja;
2) Projektowanie sieci;
3) Konfiguracja sieci;
4) Wdrażanie i eksploatacja sieci;

IRM vs. GRC – jak radzą sobie organizacje?

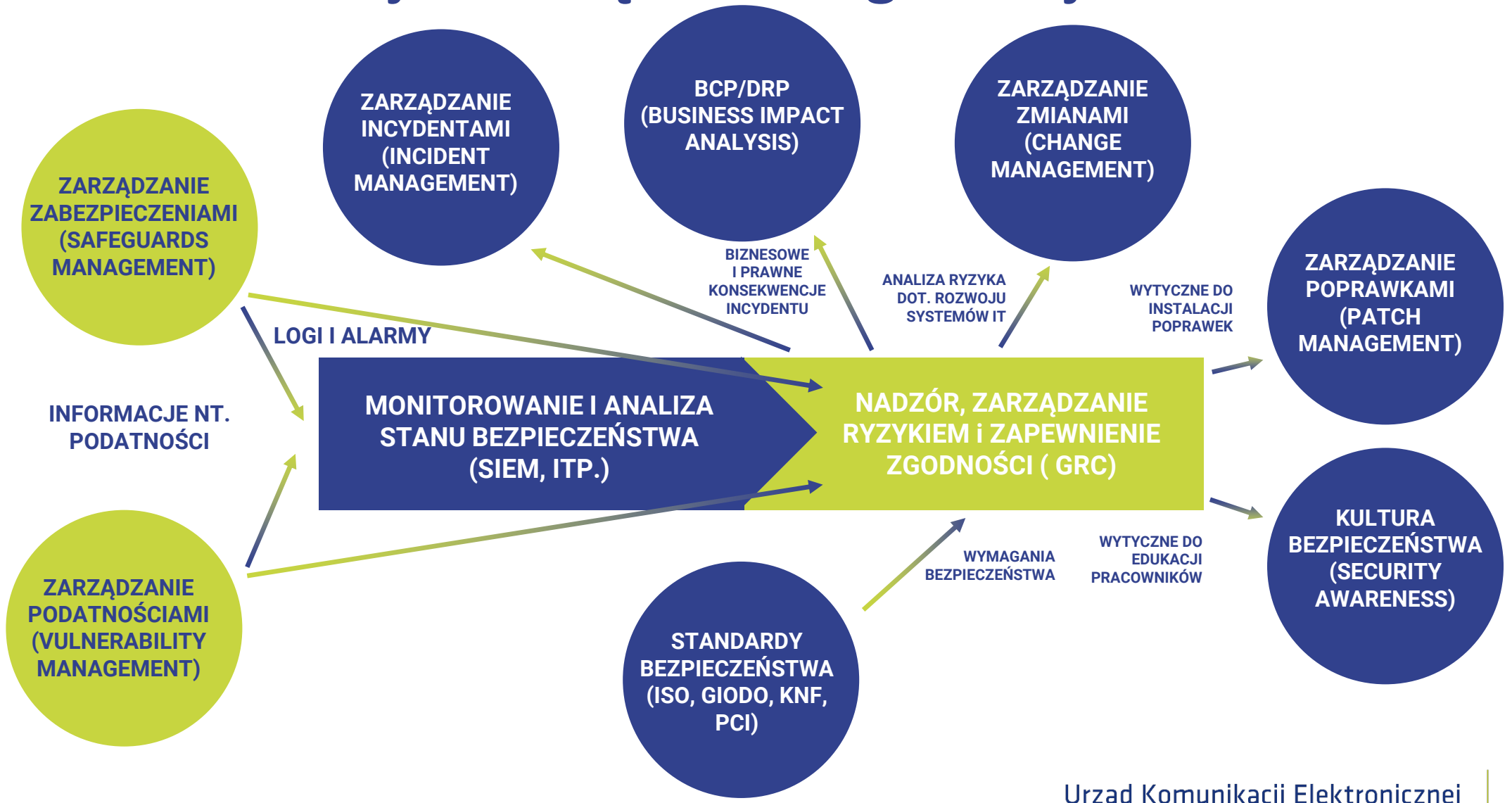


(GARTNER INC.)

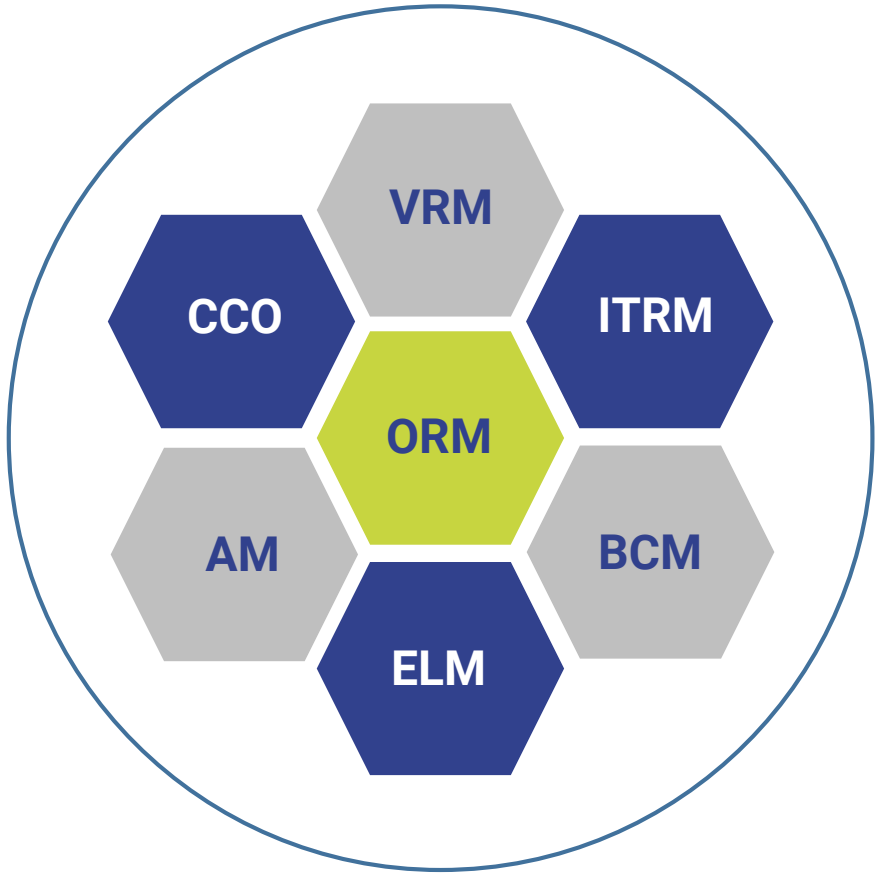
W ciągu ostatnich kilkunastu lat organizacje ewoluowały w zakresie korzystania z technologii, aby ulepszyć sposób zarządzania ryzykiem w wielu obszarach.

W szczególności radykalnie zmieniło się zarządzanie ryzykiem strategicznym, operacyjnym i informatycznym za pomocą technik informatycznych

IRM vs. GRC – jak radzą sobie organizacje?



IRM vs. GRC – jak radzą sobie organizacje?



INTEGRATED RISK MANAGEMENT

Wg firmy Gartner występuje siedem segmentów rynku w ramach szerszego rynku rozwiązań Zarządzania ryzykiem operacyjnym (ORM)

- Zarządzanie ryzykiem IT (ITRM)
- Planowanie zarządzania ciągłością biznesową (BCM)
- Zarządzanie ryzykiem dostawcy IT (VRM)
- Zgodność korporacyjna i nadzór (CCO)
- Zarządzanie audytem (AM)
- Zarządzanie prawne przedsiębiorstwa (ELM)

IRM

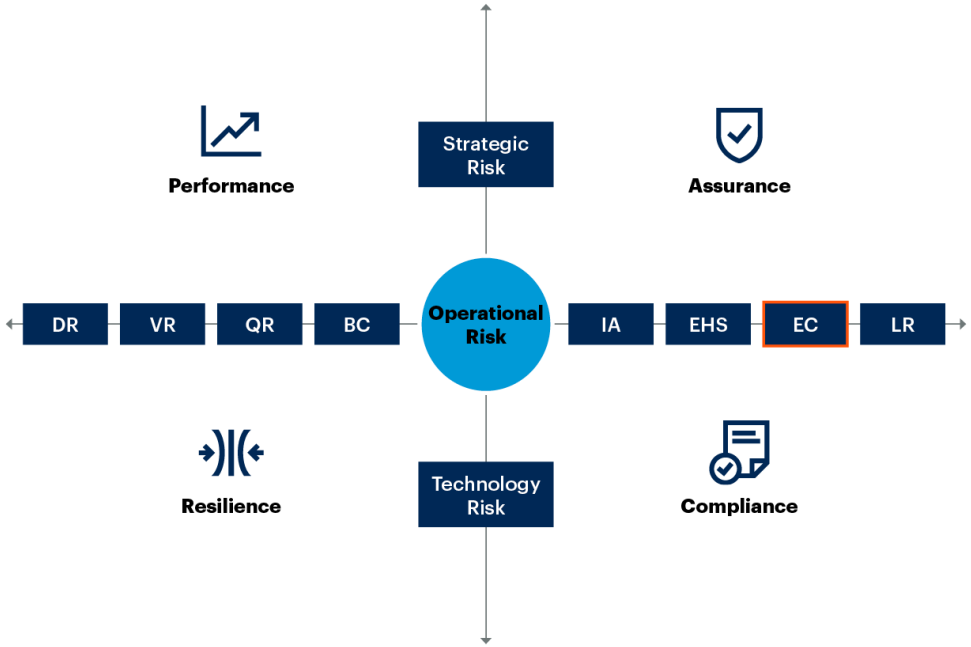
IRM to zestaw praktyk i procesów wspieranych przez kulturę świadomą ryzyka i technologie wspomagające, które usprawniają podejmowanie decyzji i wydajność poprzez zintegrowany obraz tego, jak dobrze organizacja zarządza swoim unikalnym zestawem ryzyk.

Rozwiązania IRM:

zapewniają zintegrowany wertykalnie obraz ryzyka, począwszy od strategii organizacji, poprzez jej operacje biznesowe, a na końcu do zasobów technologicznych.
IRM ma na celu zwiększenie wydajności i wartości dodanej poprzez osiąganie lepszych wyników, większej odporności, większej pewności i bardziej efektywnej zgodności dla wszystkich kluczowych interesariuszy.

Odbywa się to za pomocą szeregu zintegrowanych rozwiązań, od specjalnie zbudowanych aplikacji po zintegrowane zestawy rozwiązań jednego dostawcy w ośmiu domenach przypadków użycia i czterech celach biznesowych

Integrated Risk Management Objectives and Use-Case Domains



Source: Gartner

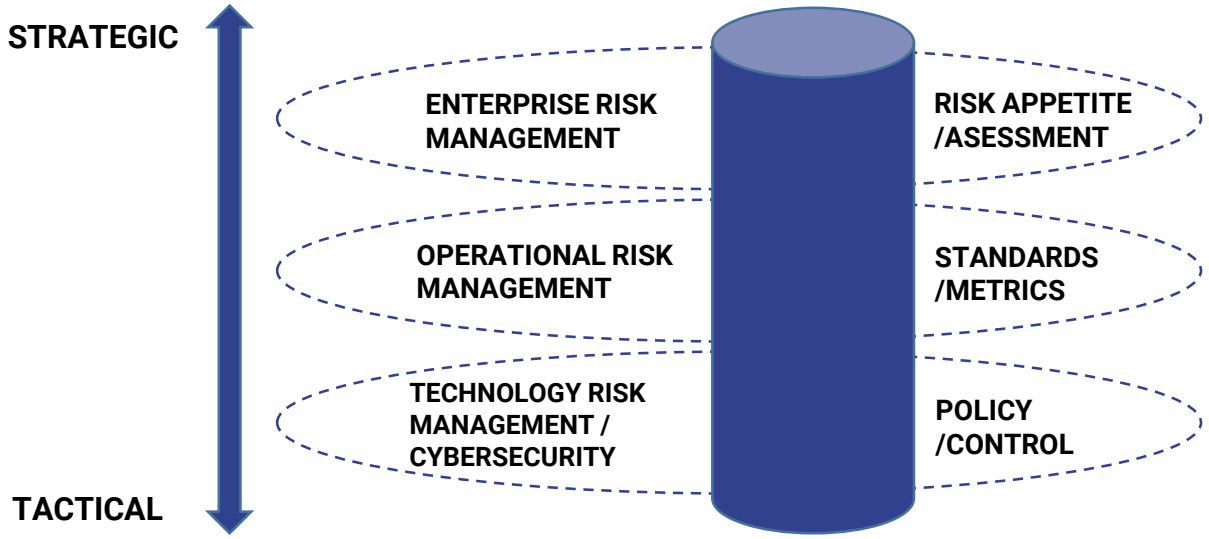
BC = business continuity; DR = digital risk; EC = ethics and compliance; EHS = environment, health and safety; IA = internal audit; LR = legal risk; QR = quality risk; VR = vendor/third-party risk

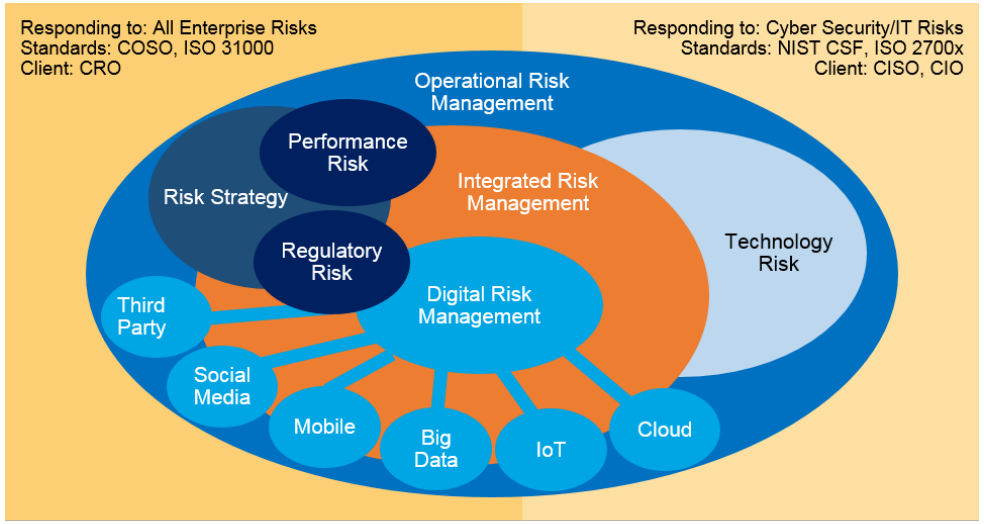
728530_C

IRM

IRM to zestaw praktyk i procesów wspieranych przez kulturę świadomą ryzyka i technologie wspomagające, które usprawniają podejmowanie decyzji i wydajność poprzez zintegrowany obraz tego, jak dobrze organizacja zarządza swoim unikalnym zestawem ryzyk.

IRM wykracza poza tradycyjną, opartą na zgodności technologię GRC, dostarczając informacji zorientowanych na działanie, zgodnych ze strategiami i wynikami biznesowymi, a nie tylko wymogami regulacyjnymi.





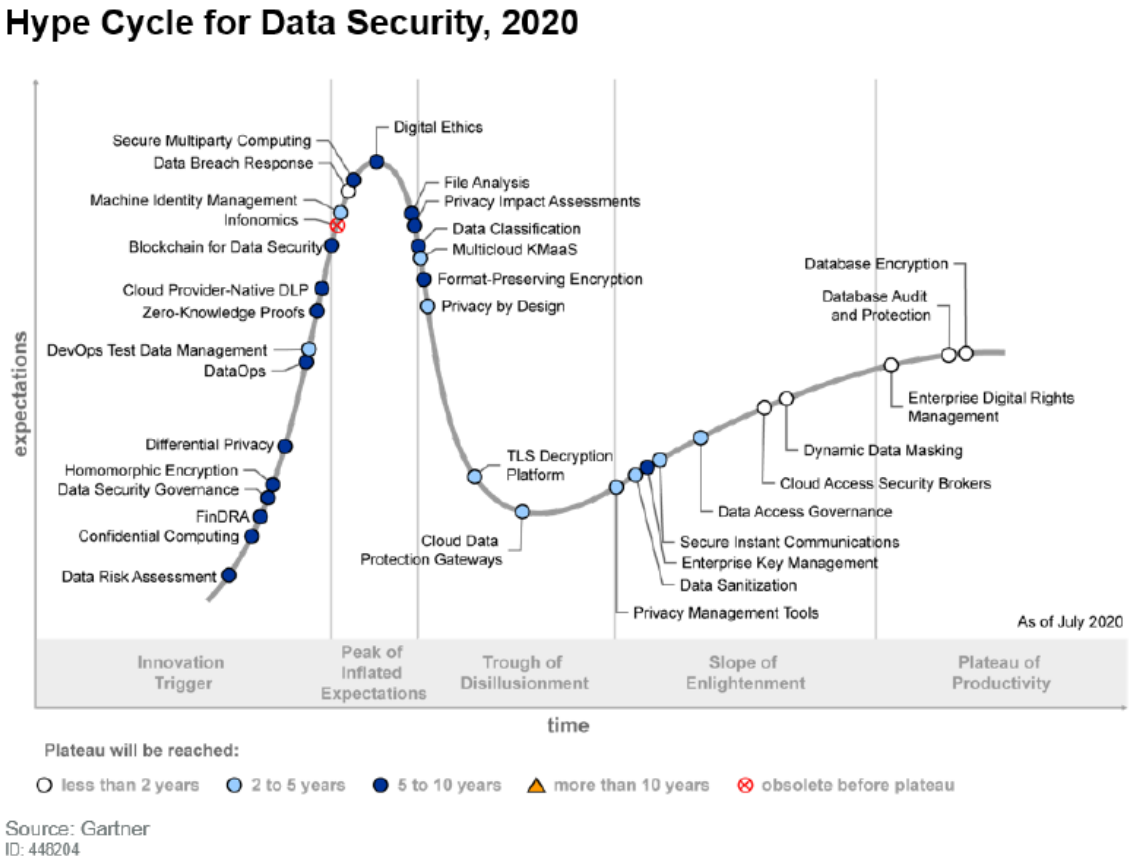
IRM

Poprzez wspólne funkcje, takie jak repozytorium aktywów, mapowanie przepisów, możliwości ankiet, funkcje przepływu pracy i import danych, dostawcy IRM obecnie zapewniają możliwości w następujących sześciu przypadkach użycia:

- **Cyfrowe zarządzanie ryzykiem (DRM)**
- **Zarządzanie ryzykiem dostawcy (VRM)**
- **Zarządzanie ciągłością biznesową (BCM)**
- **Zarządzanie audytem (AM)**
- **Zgodność korporacyjna i nadzór (CCO)**
- **Zarządzanie prawne przedsiębiorstwa (ELM)**

HYPER CYCLE – BEZPIECZEŃSTWO DANYCH

- Organizacje stoją przed ogromnymi wyzwaniami, wychodząc z skutków globalnego kryzysu 2020 r. i nowymi strategiami pracy z domu oraz szybszym wdrażaniem usług hybrydowych i usług w wielu chmurach.
- Strategia bezpieczeństwa danych musi uwzględniać rosnące zagrożenia związane z miejscem przechowywania danych, prywatnością i złośliwymi działaniami.
- Technologie i usługi związane z bezpieczeństwem operacyjnym chronią systemy IT przed atakiem poprzez identyfikację zagrożeń i narażenie na podatność, umożliwiając skuteczną reakcję i naprawę.

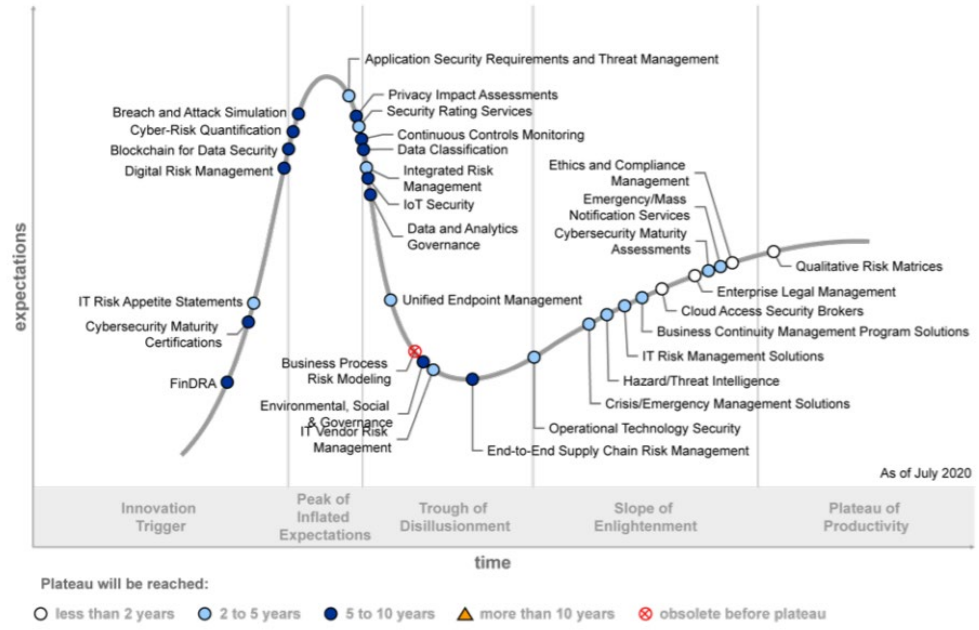


Source: Gartner
ID: 448204

HYPER CYCLE – BEZPIECZEŃSTWO DANYCH

W 2020 roku Organizacje uznają zarządzanie ryzykiem za jeden z najważniejszych priorytetów biznesowych.
Liderzy bezpieczeństwa i zarządzania ryzykiem muszą sprostać temu wyzwaniu, wyposażając kadrę kierowniczą wyższego szczebla i członków zarządu w praktyczne narzędzia i porady dotyczące zarządzania ryzykiem, na które zwrócono uwagę w tegorocznych badaniach

Hype Cycle for Risk Management, 2020



Source: Gartner
ID: 448047

Priority Matrix for Risk Management, 2020

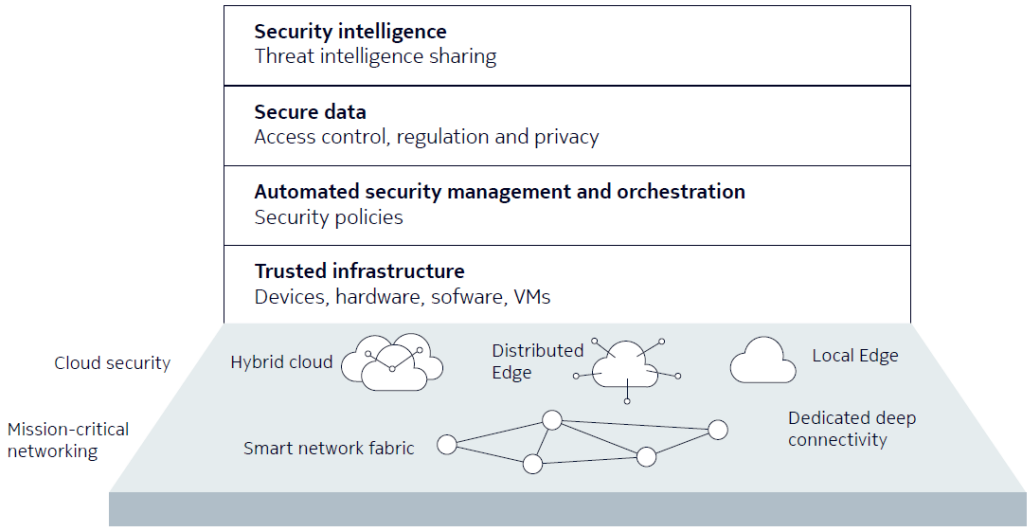
benefit	years to mainstream adoption			
	less than two years	two to five years	five to 10 years	more than 10 years
transformational		Integrated Risk Management	Digital Risk Management FinDRA	
high	Cloud Access Security Brokers Enterprise Legal Management Qualitative Risk Matrices	Application Security Requirements and Threat Management Business Continuity Management Program Solutions Crisis/Emergency Management Solutions Cybersecurity Maturity Assessments Emergency/Mass Notification Services Hazard/Threat Intelligence IT Risk Management Solutions Operational Technology Security Unified Endpoint Management	Blockchain for Data Security Breach and Attack Simulation Continuous Controls Monitoring Cyber-Risk Quantification Cybersecurity Maturity Certifications Data and Analytics Governance Data Classification End-to-End Supply Chain Risk Management Environmental, Social & Governance IoT Security Privacy Impact Assessments	
moderate	Ethics and Compliance Management	IT Risk Appetite Statements IT Vendor Risk Management Security Rating Services		
low				

As of July 2020

Source: Gartner
ID: 448047

IMPLEMENTACJA 5G – ZAGROŻENIA / BEZPIECZEŃSTWO

- Funkcje bezpieczeństwa 5G są bardziej zorientowane na potrzeby operatorów niż przedsiębiorstw i mogą nie spełniać wszystkich wymagań przedsiębiorstwa.
- Złożoność i niesprawdzony charakter 5G może wprowadzić nowe zagrożenia
- Należy więc dyskutować o całym ekosystemie bezpieczeństwa w układzie np. 4 warstw bezpieczeństwa (źródło: Nokia)



WSPÓLNE NURTY

Bezpieczeństwo cyfrowe (bezpieczeństwo systemów IT / ICT) jest kompleksem działań opartych o analizę ryzyka i niezbędne narzędzia analityczne obejmującym cały proces zapewniania bezpieczeństwa począwszy od procesu standaryzacji (kreowania wizji technicznej i organizacyjnej biznesu/systemu), poprzez bezpieczny i transparentny proces wytwarzania, po narzędzia operacyjne zarządzania ryzykiem i bezpieczeństwem występującym w systemach IT/ ICT