ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Bezpieczna migracja do chmury

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Marcin Fronczak

Prowadzi szkolenia z zakresu bezpieczeństwa chmur m.in. przygotowujące do egzaminu Certified Cloud Security Knowledge (CCSK). Certyfikowany audytor systemów informatycznych oraz ekspert w zarządzaniu ryzykiem i bezpieczeństwem informacji - CISA, CIA, CRISC.

ZAUFANA TRZECIA STRONA.PL

Agenda

aruba CLOUD

1. Podsumowanie zagadnień poruszanych w poprzednich artykułach
2. Proces migracji krok po kroku z punktu widzenia bezpieczeństwa
3. Podsumowanie
4. Sesja pytań od uczestników

ZAUFANA TRZECIA STRONA.PL

Podsumowanie zagadnień

aruba CLOUD

- architektura modelu cloud computingu wg NIST SP 800-145,
- ryzyka natury organizacyjno-prawnej i zarządzania zgodnością na przykładzie pojęcia GRC – Governance, Risk management and Compliance,
- wymagania prawne,
- standardy bezpieczeństwa i audyt w chmurze
- RODO w chmurze,
- zarządzanie tożsamością w chmurze i standardy SAML, OpenID, OAuth,
- wdrożenie i zarządzanie uprawnieniami w chmurze,
- przygotowania do wielkiej awarii,
- bezpieczeństwo centrum danych,
- bezpieczeństwo środowiska wirtualnego,
- szyfrowanie w chmurze,
- zarządzanie incydentami w chmurze,
- interoperacyjność i przenaszalność – jak uniezależnić się od dostawcy,
- zarządzanie cyklem życia bezpieczeństwa danych (datasecurity lifecycle),
- Secure Software Development Cycle,
- zarządzanie relacjami z dostawcą
- Security as a Service

ZAUFANA TRZECIA STRONA.PL

Bank w chmurze?

aruba CLOUD

- Styczeń 2018 – Lloyd's szacuje straty wynikające z awarii usług chmurowych w USA na około 19 miliardów dolarów.
- Czerwiec 2018 – Lloyd's podpisuje wart 1,2 miliarda funtów, 10-letni kontrakt z IBM na dostarczenie usług chmurowych i migrację bankowych systemów do chmury

ZAUFANA TRZECIA STRONA.PL

Scenariusz migracji

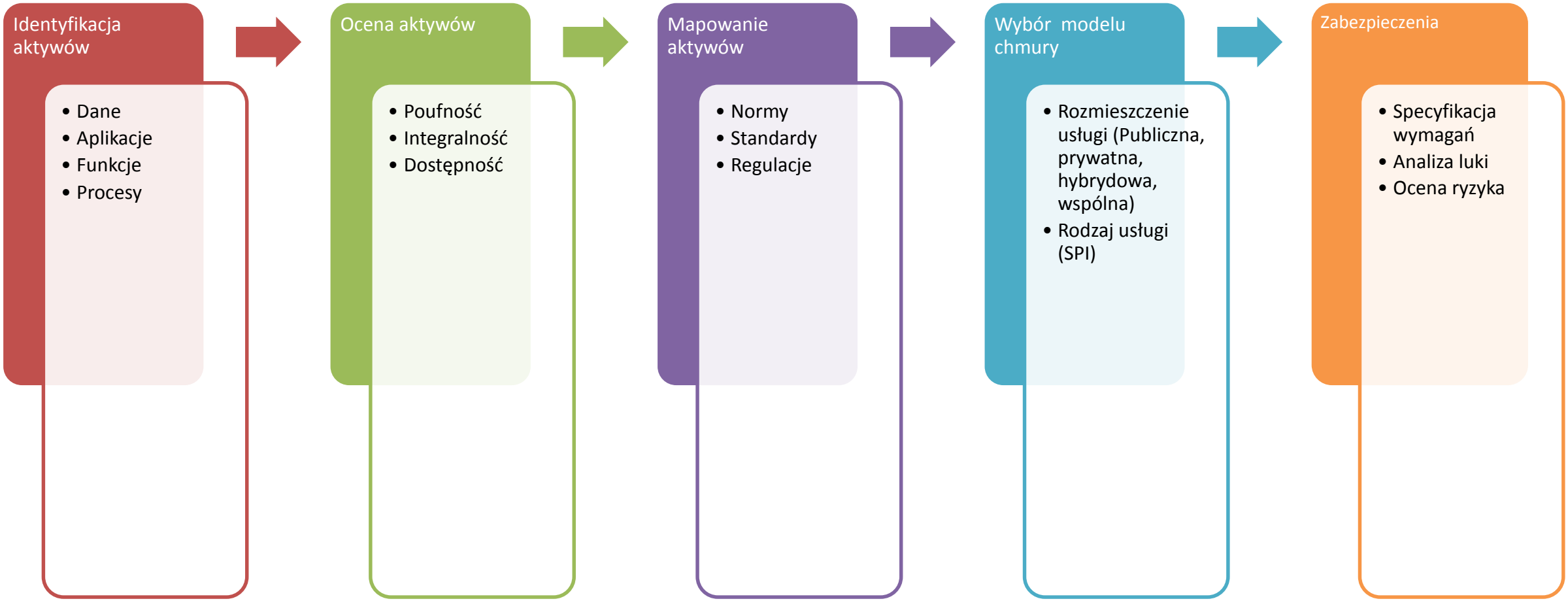
aruba CLOUD

- Korzystamy z usługi w modelu platform as a service (PaaS) do rozwoju aplikacji
- Aplikacja do szacowania zdolności kredytowych potencjalnych klientów
- Zintegrowana z wewnętrznymi systemami bankowymi
- Przetwarza dane osobowe
- Uruchamiana okresowo

ZAUFANA TRZECIA STRONA.PL

Migracja do chmury

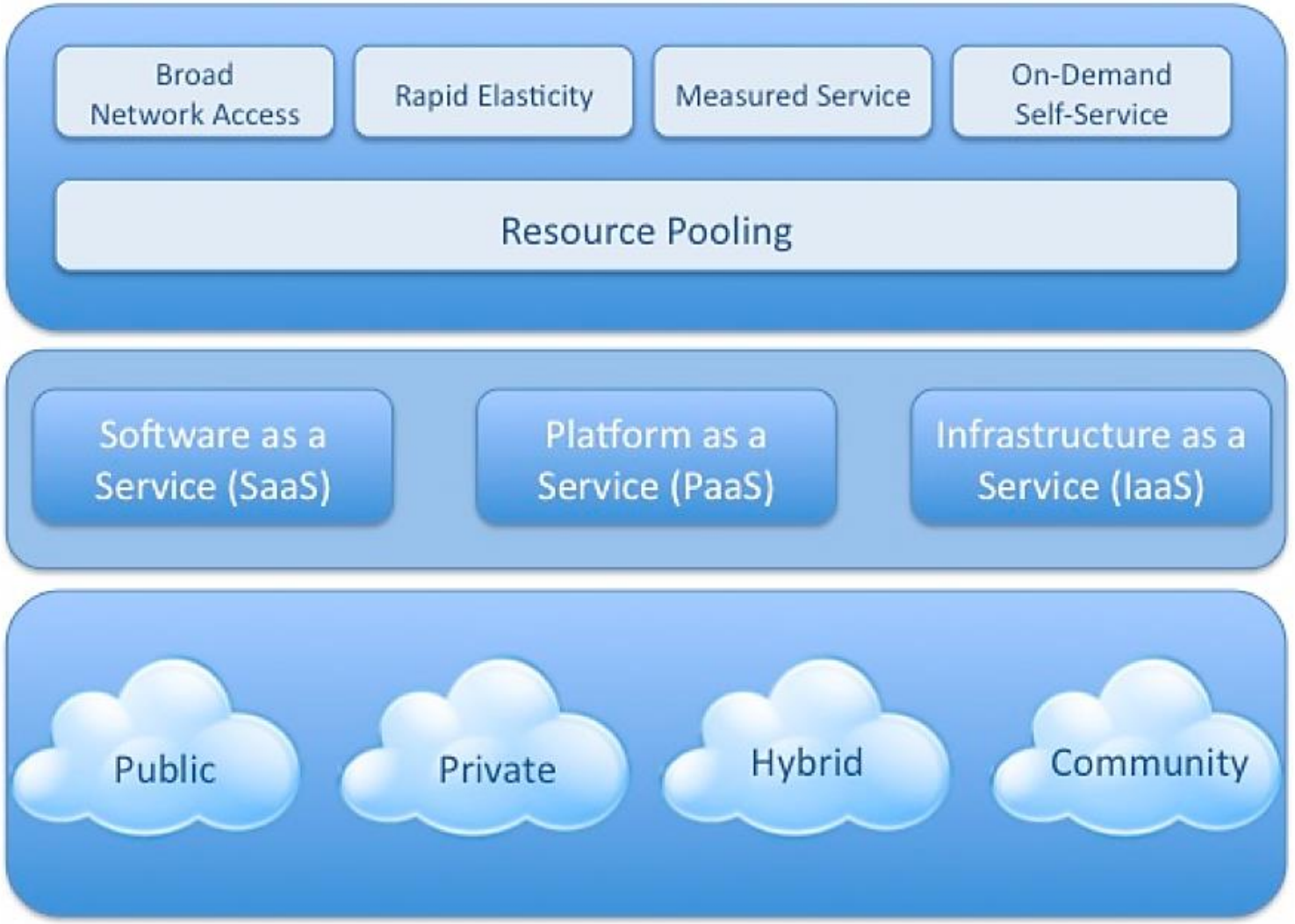
aruba CLOUD



ZAUFANA TRZECIA STRONA.PL

Model chmury wg NIST

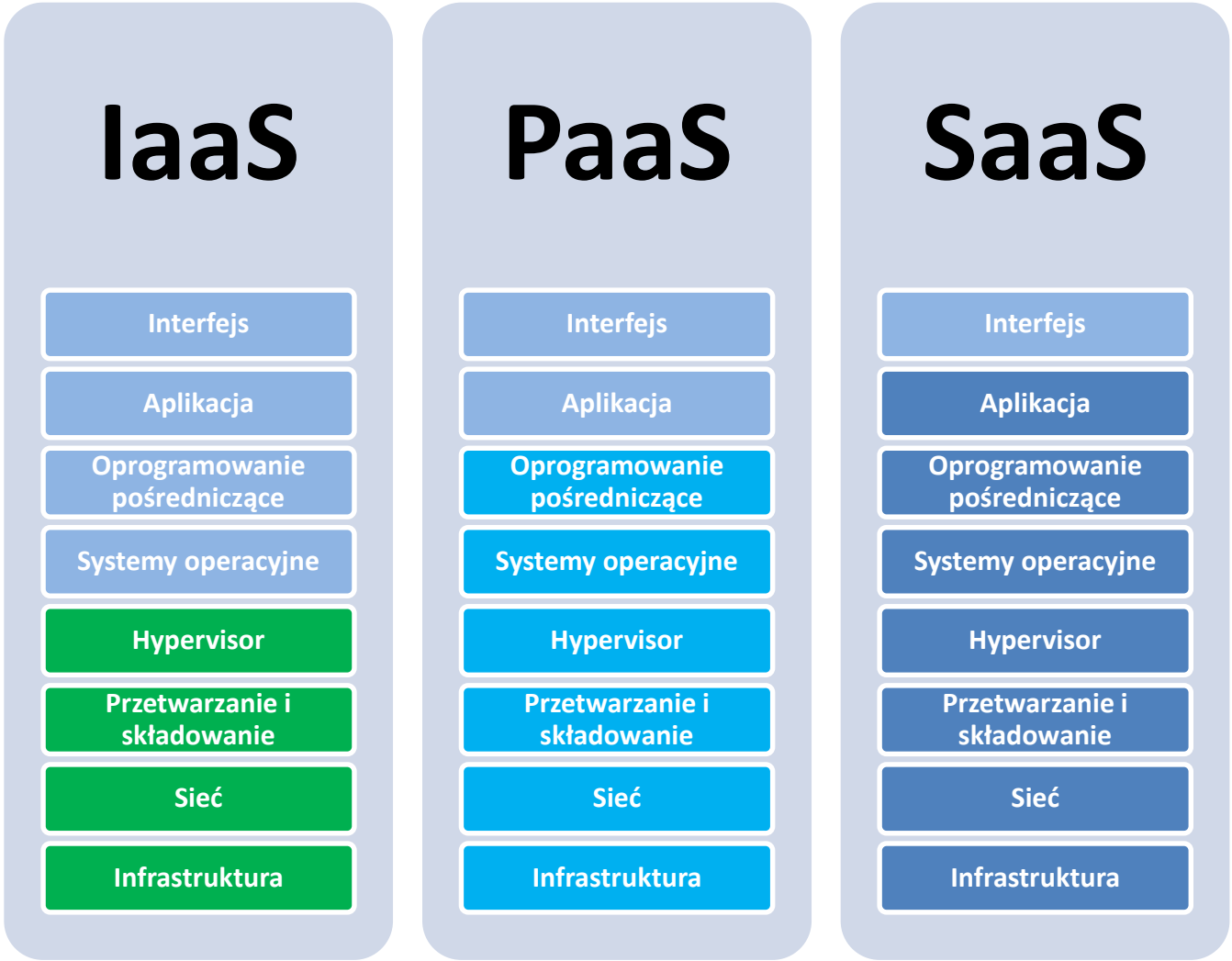
aruba CLOUD



ZAUFANA TRZECIA STRONA.PL

Stos SPI

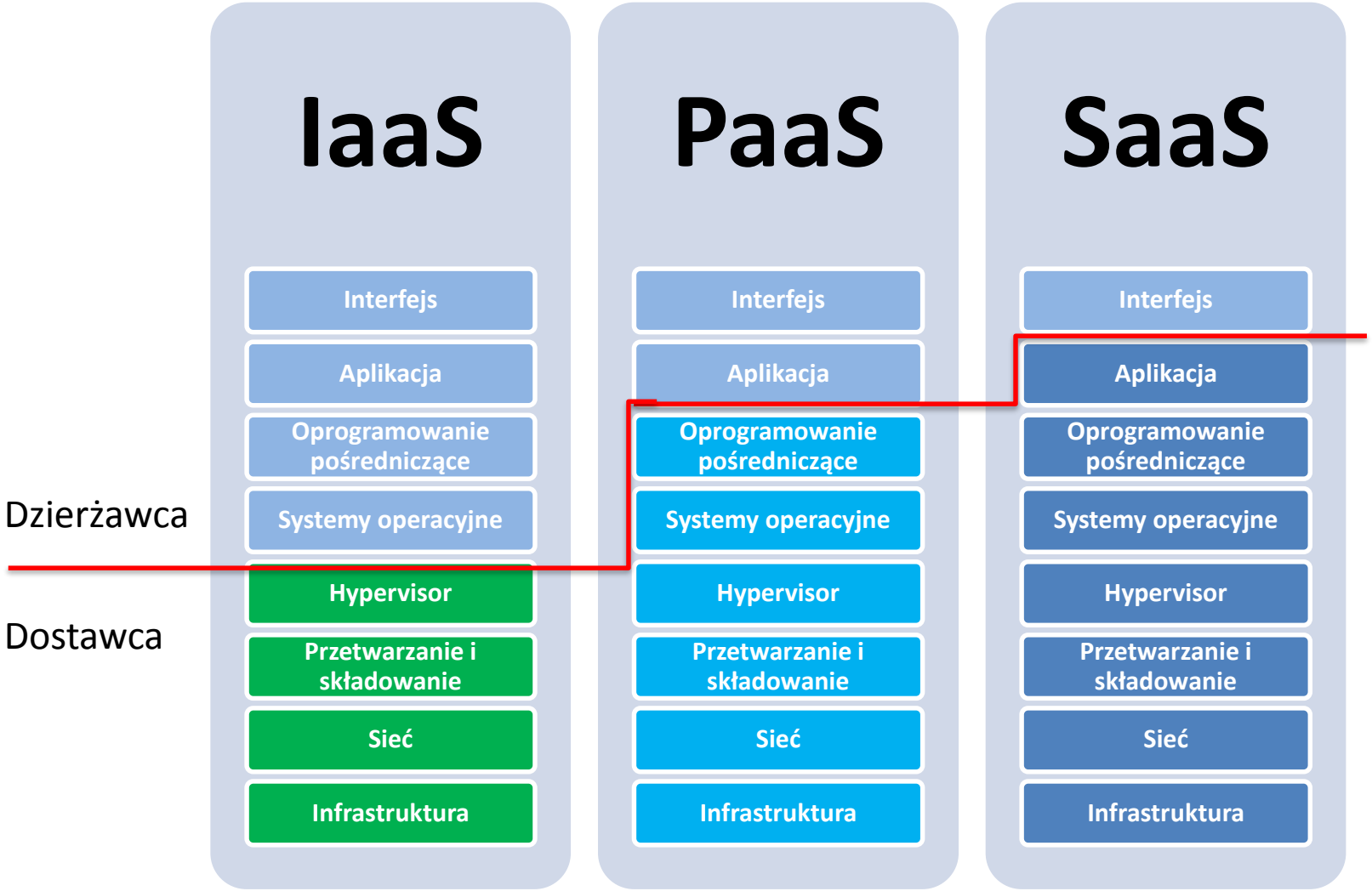
aruba CLOUD



ZAUFANA TRZECIA STRONA.PL

Podział odpowiedzialności

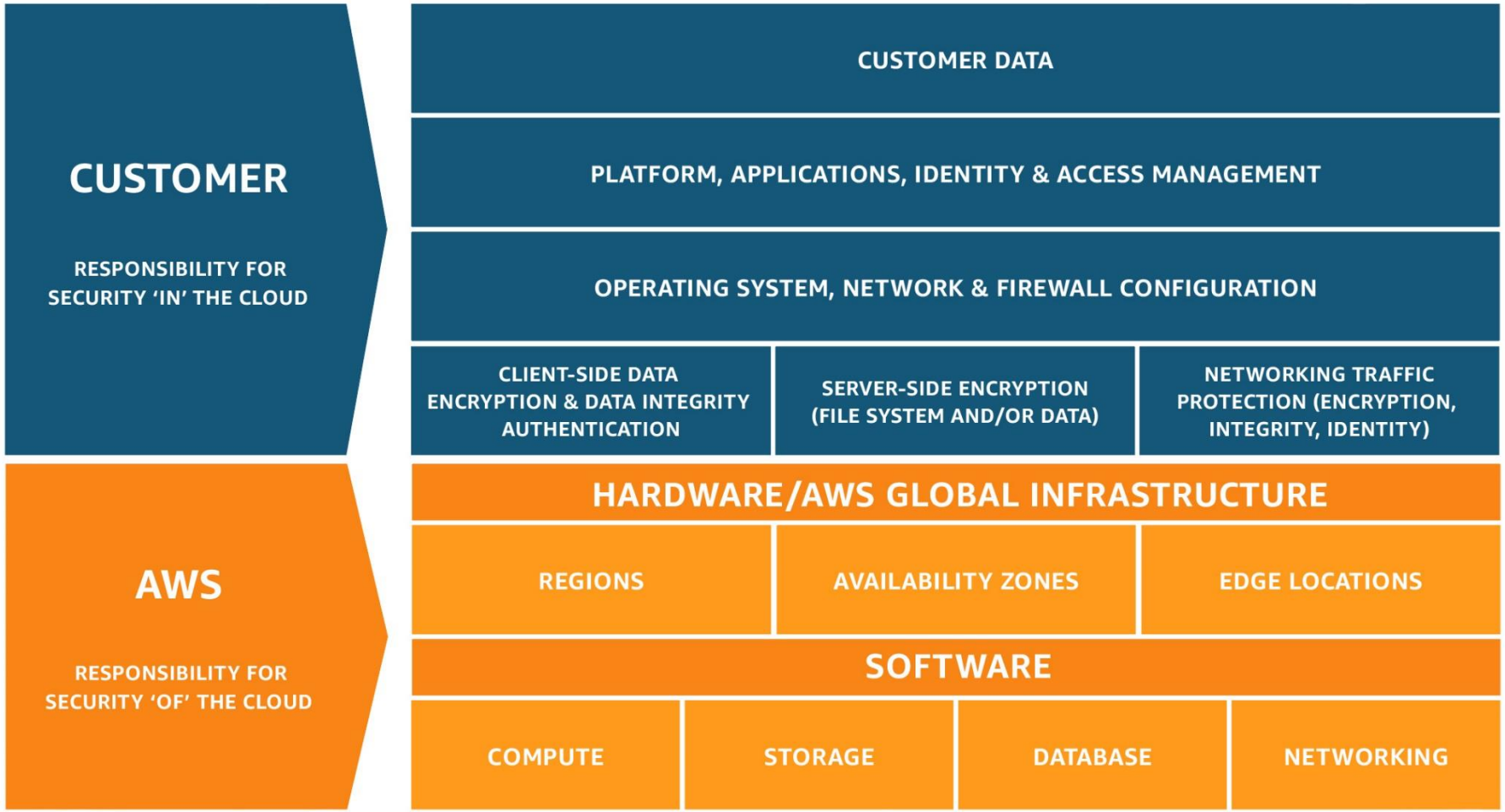
aruba CLOUD



ZAUFANA TRZECIA STRONA.PL

Podział odpowiedzialności

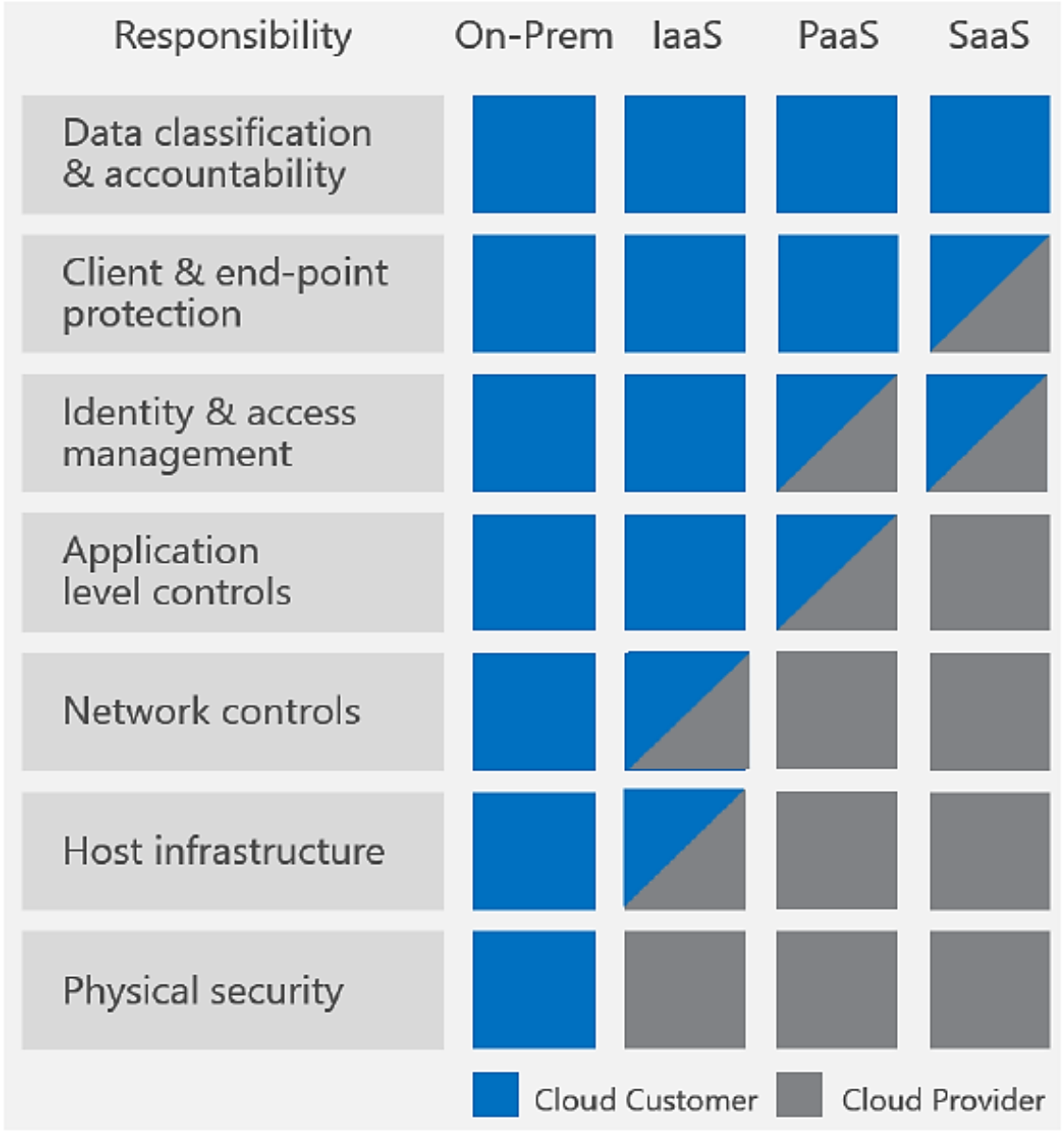
aruba CLOUD



ZAUFANA TRZECIA STRONA.PL

Podział odpowiedzialności

aruba CLOUD



ZAUFANA TRZECIA STRONA.PL

Podział odpowiedzialności

aruba CLOUD

	Infrastruktura zarządzana przez:	Infrastruktura w posiadaniu:	Infrastruktura umieszczona:	Dostępna i wykorzystywana przez:
Publiczna	Dostawca (Third Party Provider)	Dostawca (Third Party Provider)	Na zewnątrz (Off-Premise)	Niezaufana strona
Prywatna/ Współdzielona	Organizacja Lub Dostawca	Organizacja Dostawca	Wewnątrz (On-Premise) Na zewnątrz	Zaufana strona
Hybrydowa	Zarówno Organizacja jak i Dostawca	Zarówno Organizacja jak i Dostawca	Zarówno Wewnątrz jak i Na zewnątrz	Zarówno Zaufana i Niezaufana strona

ZAUFANA TRZECIA STRONA.PL

Podział odpowiedzialności

aruba CLOUD

Bezpieczeństwo	Interfejs	Prywatna (On-Premise)	Prywatna (Off-Premise)	Public		
				IaaS	PaaS	SaaS
Personel	Odbiorca	Odbiorca	Wspólna	Wspólna	Wspólna	Dostawca
Bezpieczeństwo aplikacji	Odbiorca	Odbiorca	Odbiorca	Odbiorca	Odbiorca	Dostawca
Zarządzanie dostępem i tożsamością	Odbiorca	Odbiorca	Odbiorca	Odbiorca	Odbiorca	Dostawca
Zarządzanie logami	Odbiorca	Odbiorca	Odbiorca	Odbiorca	Odbiorca	Dostawca
Szyfrowanie danych	Odbiorca	Odbiorca	Odbiorca	Odbiorca	Odbiorca	Dostawca
Host Intrusion Detection	Odbiorca	Odbiorca	Odbiorca	Odbiorca	Dostawca	Dostawca
System monitoring	Odbiorca	Odbiorca	Odbiorca	Wspólna	Dostawca	Dostawca
OS Hardening	Odbiorca	Odbiorca	Odbiorca	Wspólna	Dostawca	Dostawca
Network Intrusion Detection	Odbiorca	Odbiorca	Dostawca	Dostawca	Dostawca	Dostawca
Bezpieczeństwo sieci	Odbiorca	Odbiorca	Dostawca	Dostawca	Dostawca	Dostawca
Polityki bezpieczeństwa	Odbiorca	Odbiorca	Dostawca	Dostawca	Dostawca	Dostawca
Bezpieczeństwo fizyczne/środ.	Odbiorca	Odbiorca	Dostawca	Dostawca	Dostawca	Dostawca

ZAUFANA TRZECIA STRONA.PL

Wpływ na bezpieczeństwo

aruba CLOUD

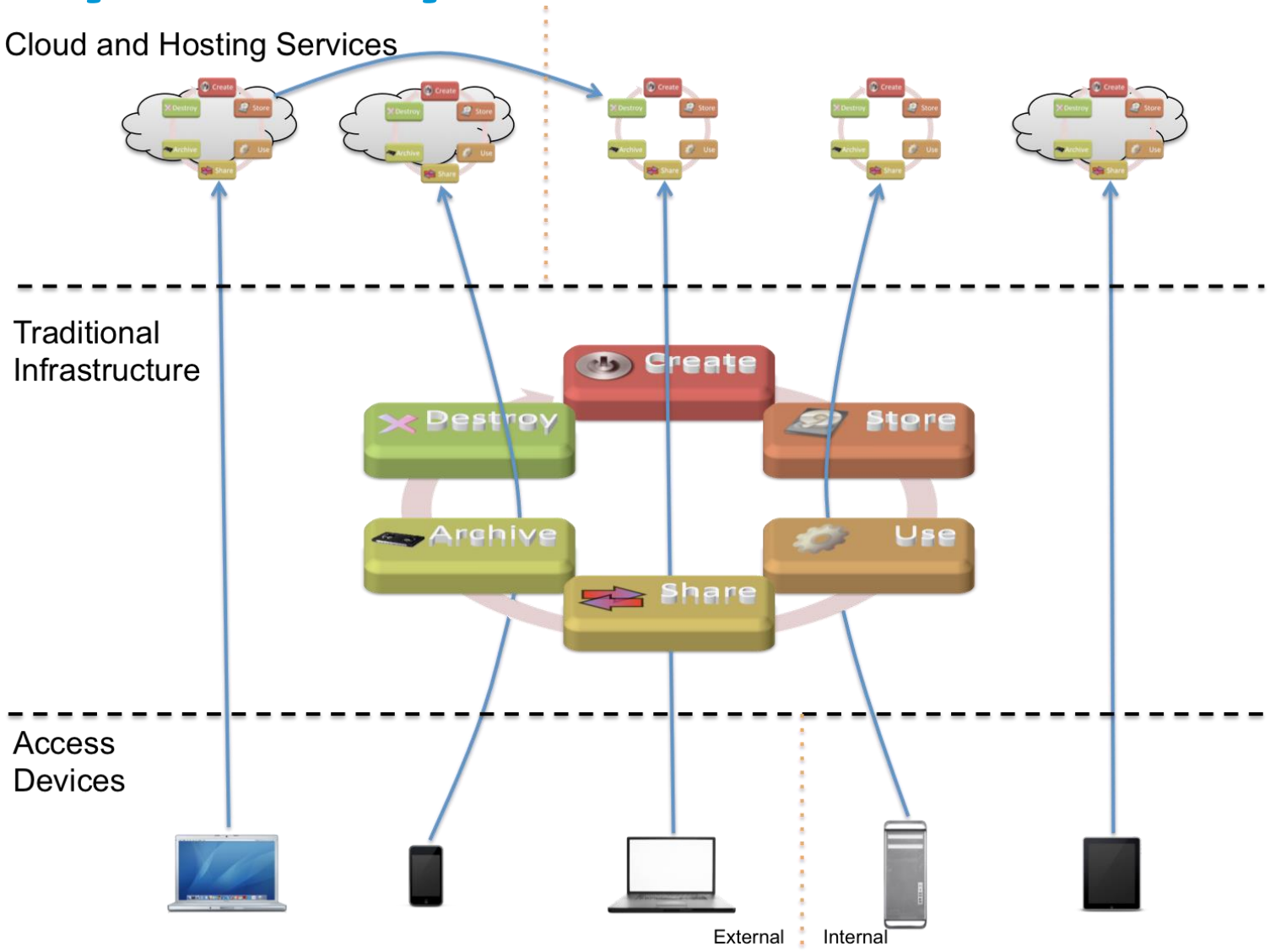
Interfejs	Mały wpływ na zabezpieczenia. Wysoka istotność dobrze skonstruowanej umowy. Monitoring usług. Raporty zgodności i z testów.
Aplikacja	
Oprogramowanie pośredniczące	Większy wpływ na zabezpieczenia. Duża istotność dobrze skonstruowanej umowy. Dobrze zaprojektowane i udokumentowane API. Monitoring usług. Raporty zgodności i z testów.
Systemy operacyjne	
Hypervisor	Duży wpływ na zabezpieczenia. Możliwość przeniesienia istniejących rozwiązań. Duża istotność dobrze skonstruowanej umowy. Dobrze zaprojektowane i udokumentowane API. Raporty zgodności i z testów.
Przetwarzanie i składowanie	
Sieć	
Infrastruktura	
Public	Niska elastyczność i możliwość negocjacji umowy. Konieczne wykorzystanie alternatywnych rozwiązań. Standardowe rozwiązania.
Private	Większa elastyczność i możliwość negocjacji umowy. Dokładny opis usługi
Hybrid & Community	Hybrydowa (chmura-chmura, chmura-centrum danych)– strategia nadzoru musi obejmować podział odpowiedzialności za wykorzystywane usługi pomiędzy klienta i dostawcę lub dostawców Współdzielona – Uwzględnienie relacji pomiędzy podmiotami w ramach grupy.

Cykl życia danych

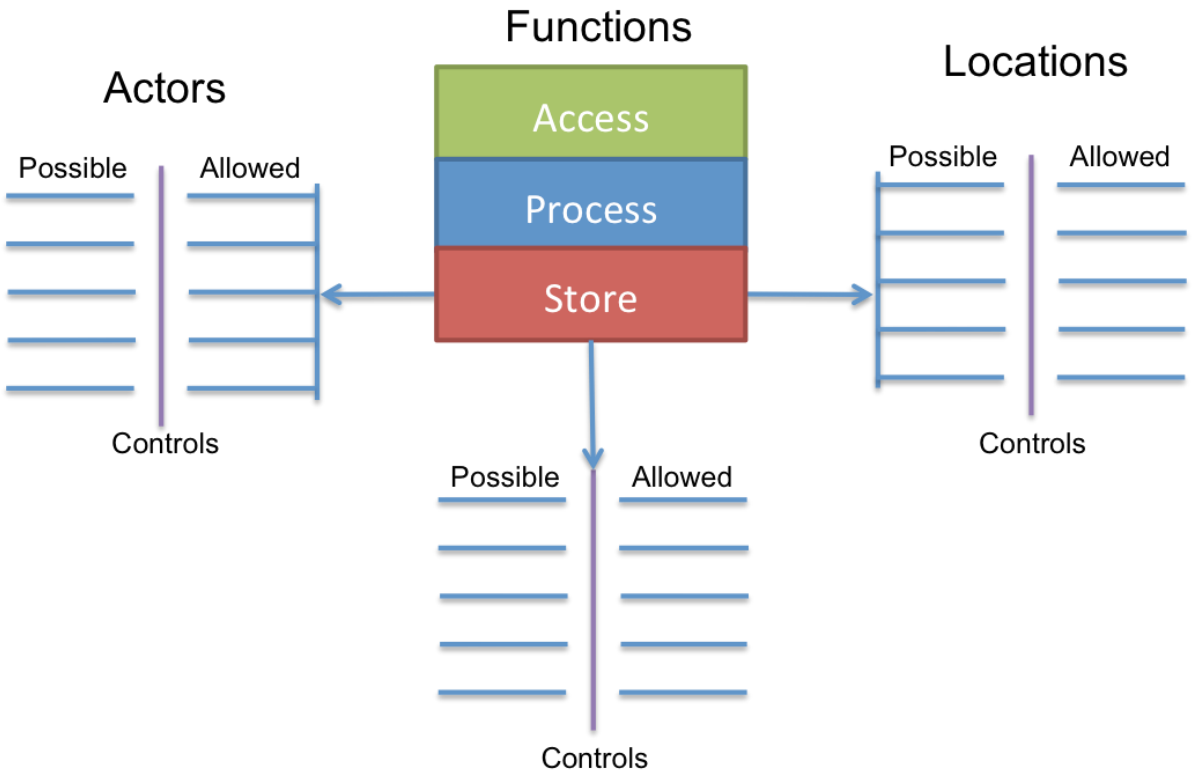
1. Wytworzenie lub zmiana/aktualizacja, modyfikacja danych w postaci cyfrowej
2. Przechowywanie jest działaniem mającym na celu składowanie danych w repozytorium i występuje zazwyczaj równolegle z procesem tworzenia
3. Korzystanie obejmuje przeglądanie, przetwarzanie i wszelkie działania wyłączając modyfikację
4. Dzielenie polega na udostępnieniu informacji innym użytkownikom , klientom, partnerom
5. Archiwizacja umożliwia dostęp i korzystanie z danych w zdefiniowanym okresie czasu
6. Niszczenie polega na całkowitym usunięciu danych przy wykorzystaniu fizycznych lub logicznych środków.

Cykl życia danych

- Gdzie są moje dane?
- Kto ma do nich dostęp?
- Z jakich urządzeń?
- Jakie działania może na nich wykonać?
- Czy można przenosić dane pomiędzy lokalizacjami?
- Jaki jest cykl życia danych w tych lokalizacjach?



Cykl życia danych



	Create	Store	Use	Share	Archive	Destroy
Access	X	X	X	X	X	X
Process	X		X			
Store		X			X	

Funkcje

Access: Przegląd/dostęp do danych, kopiowanie, przesyłanie, wymiana informacji

Process: Operacje na danych jak aktualizacja, transakcje biznesowe itd.

Store: Przechowywanie danych (w plikach, bazach danych, hurtowniach itd.)

Aktorzy

Użytkownicy, konta systemowe, aplikacje, urządzenia

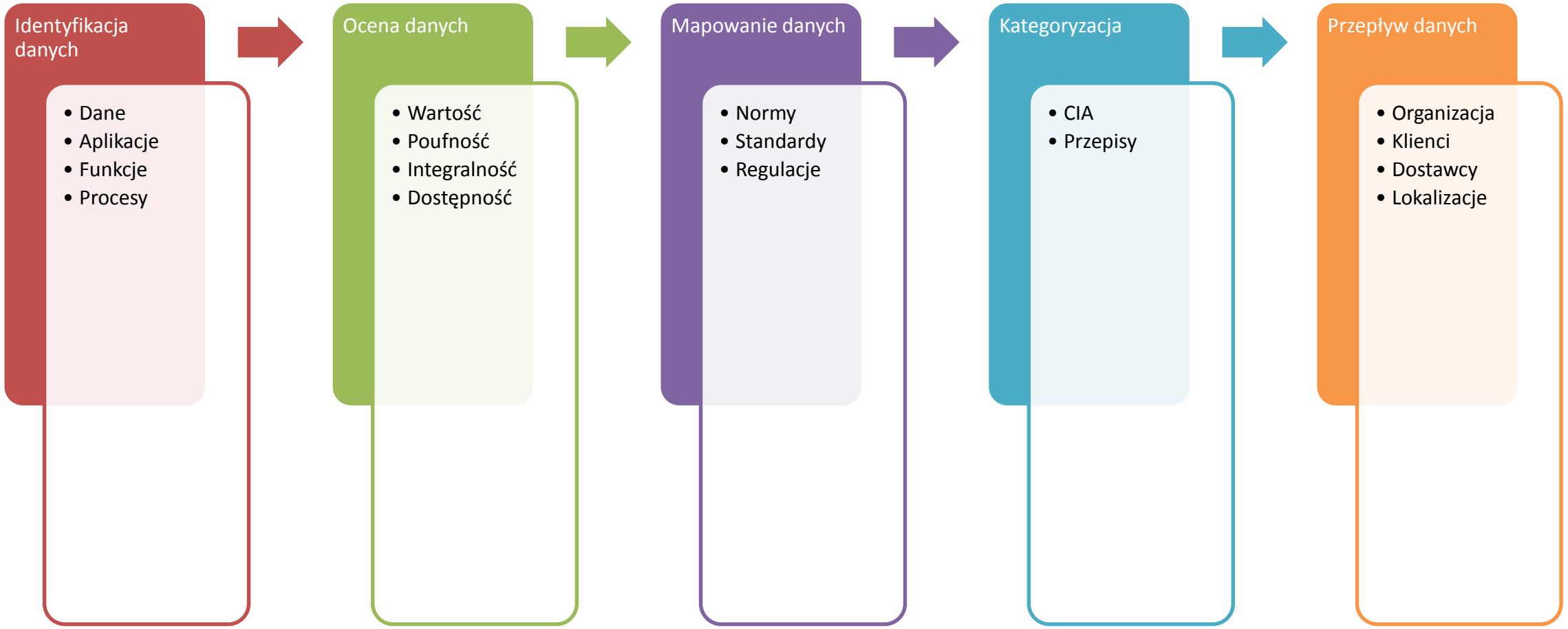
Lokalizacje

model (on-premise, chmura, zewnętrzne), geograficzne, warstwa chmury, środowisko.

ZAUFANA TRZECIA STRONA.PL

Klasyfikacja

aruba CLOUD



ZAUFANA TRZECIA STRONA.PL

Mapowanie standardów

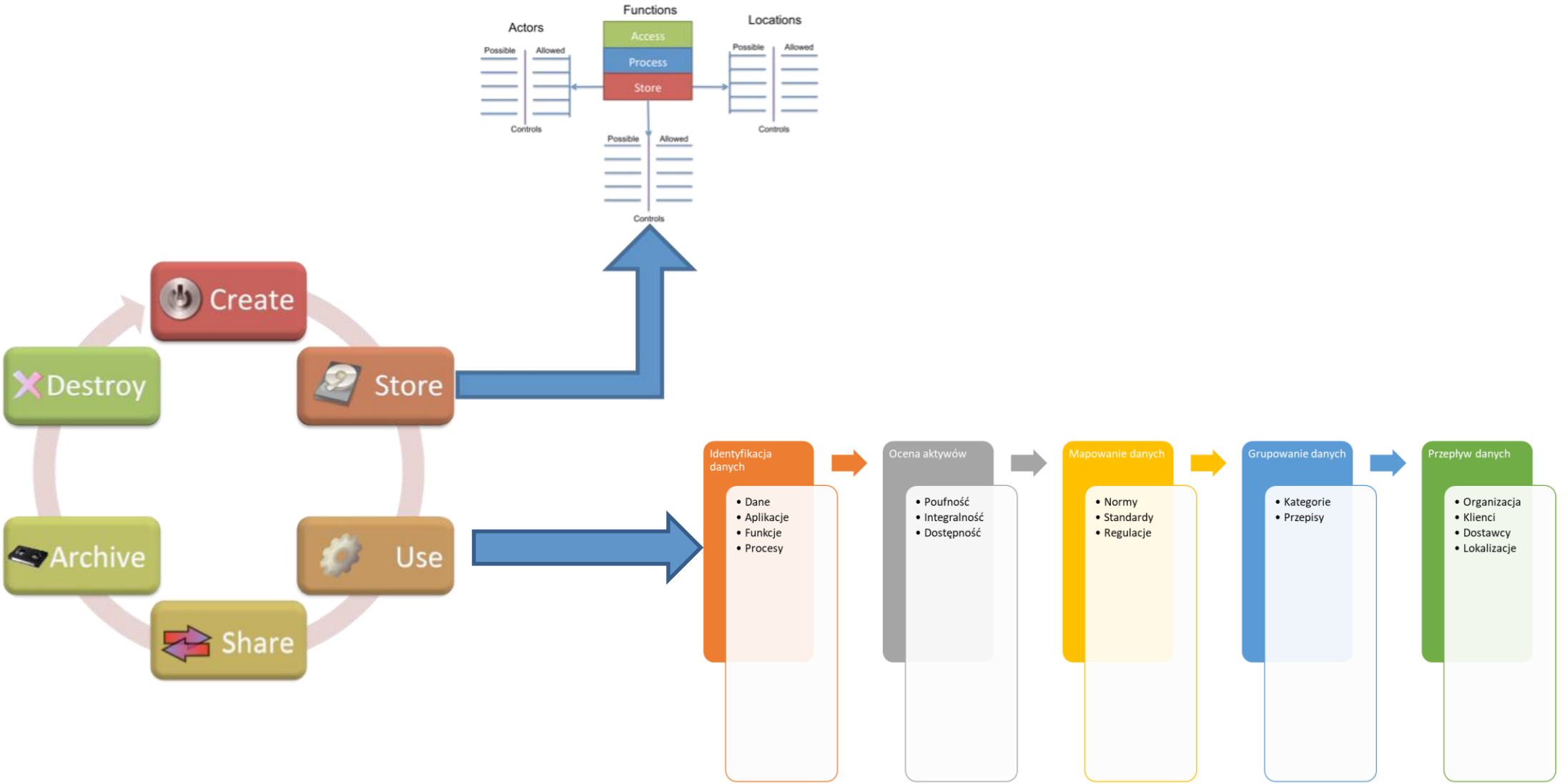
aruba CLOUD

- RODO - do 10 000 000 EUR lub 2% całkowitego rocznego światowego obrotu z poprzedniego roku (decyduje wartość wyższa) i do 20 000 000 EUR lub 4% całkowitego rocznego światowego obrotu z poprzedniego roku.
- Krajowy System Cyberbezpieczeństwa - do 200 tys. zł (a w wyjątkowych przypadkach do 1 mln zł).
- Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach (Rekomendacja 20)
- Komunikat Urzędu Komisji Nadzoru Finansowego dotyczący korzystania przez podmioty nadzorowane z usług przetwarzania danych w chmurze obliczeniowej

ZAUFANA TRZECIA STRONA.PL

Mapowanie

aruba CLOUD



ZAUFANA TRZECIA STRONA.PL

Mapowanie

aruba CLOUD

Kategoria	Funkcje	Aktorzy								Lokalizacja									
		Admin		Internal		Aplikacja		External		SaaS		PaaS		Iaas		EU		Non EU	
	Możliwe(M)/ Dopuszczalne (D)	M	D	M	D	M	D	M	D	M	D	M	D	M	D	M	D	M	D
Dane osobowe	Access	✓	✓	✓	✓	×	×	✓	×	×	✓*	×	✓*	×	✓*	✓	✓	✓	×
	Process	✓	✓	✓	✓	×	×	✓	✓	×	✓*	×	✓*	×	✓*	✓	✓	✓	×
	Store	✓	✓	✓	✓	✓	✓	×	×	×	✓*	×	✓*	×	✓*	✓	✓	✓	×

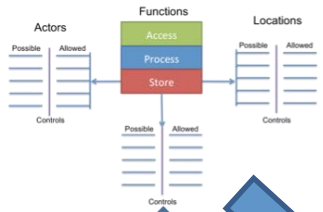
*Dopuszczalne pod warunkiem spełnienia określonych wymagań

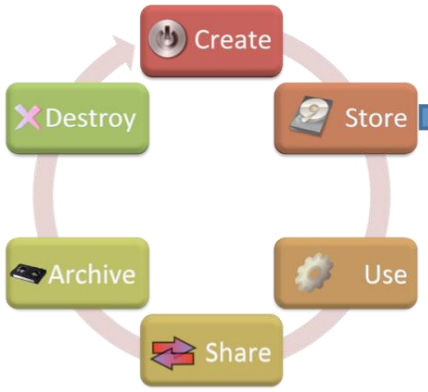
	Create	Store	Use	Share	Archive	Destroy
Access	X	X	X	X	X	X
Process	X		X			
Store		X			X	

ZAUFANA TRZECIA STRONA.PL zenia

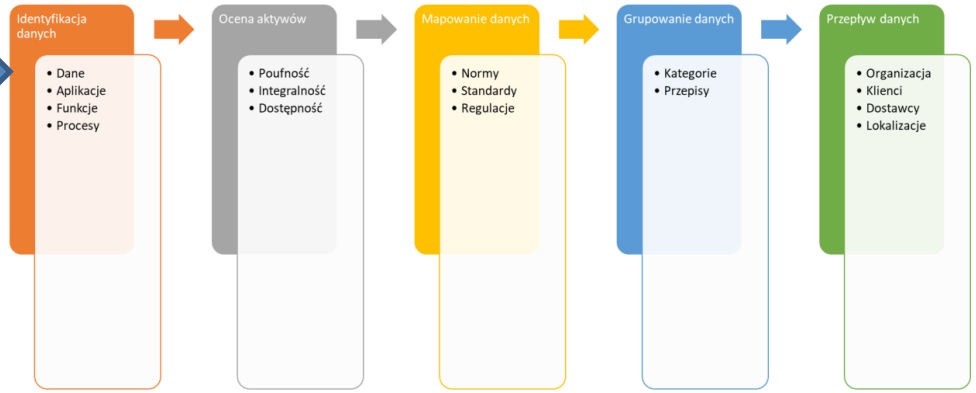
Mapowanie

aruba CLOUD





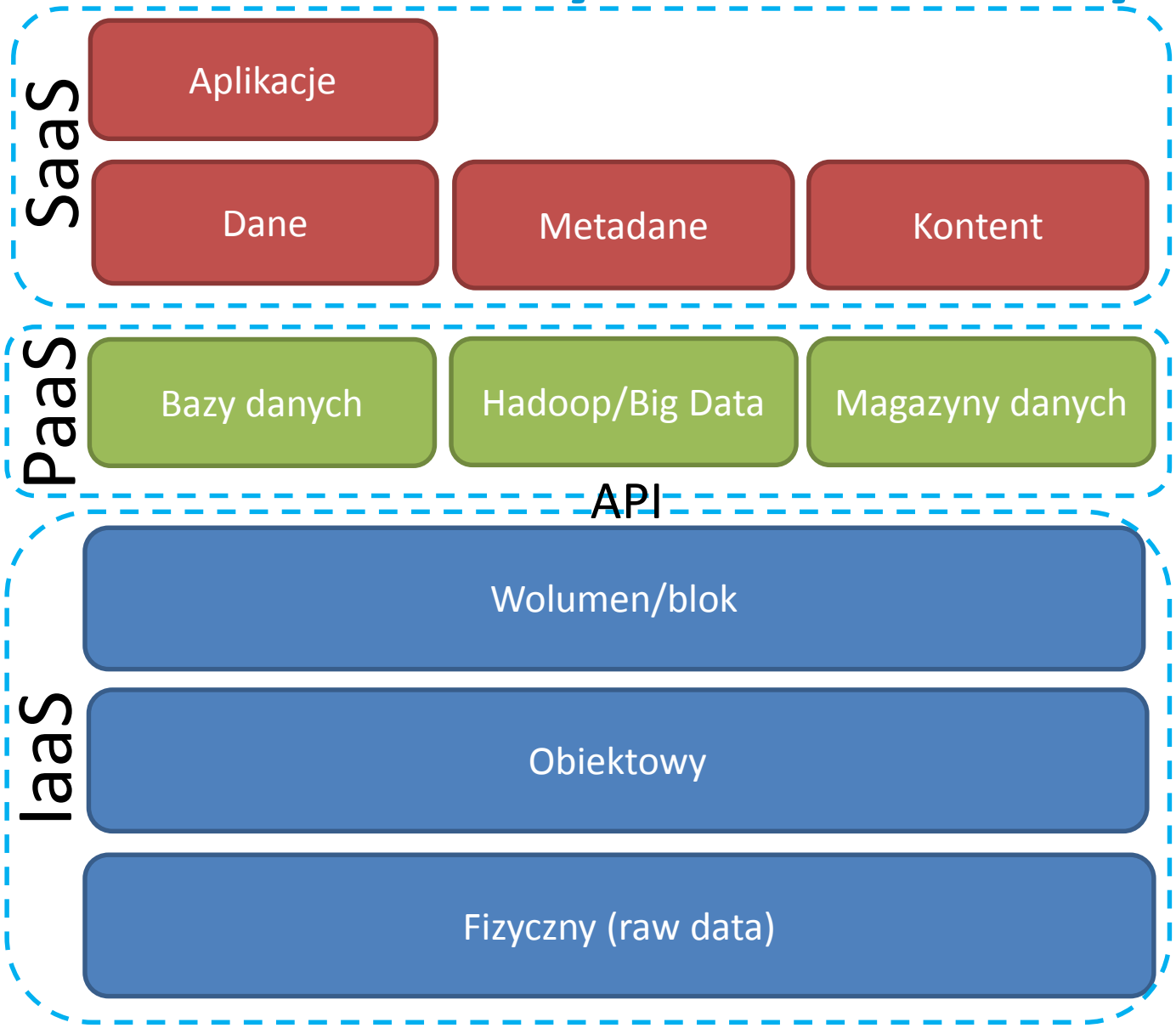
Kategoria	Funkcje	Aktorzy								Lokalizacja									
		Admin		Internal		Aplikacja		External		SaaS		PaaS		Iaas		EU		Non EU	
	Możliwe(M)/ Dopuszczalne (D)	M	D	M	D	M	D	M	D	M	D	M	D	M	D	M	D	M	D
Dane osobowe	Access	✓	✓	✓	✓	×	×	✓	×	×	✓	×	✓	×	✓	✓	✓	✓	
	Process	✓	✓	✓	✓	×	×	✓	✓	×	✓	×	✓	×	✓	✓	✓	✓	×
	Store	✓	✓	✓	✓	✓	✓	×	×	×	✓	×	✓	×	✓	✓	✓	✓	×



ZAUFANA TRZECIA STRONA.PL

Szyfrowanie danych w spoczynku

aruba CLOUD



- Provider-managed encryption: Dane są szyfrowane w aplikacji i generalnie zarządzane przez dostawcę
- Proxy encryption: Dane przechodzą przez szyfrujące proxy zanim trafią do SaaS.

- Szyfrowanie warstwy aplikacyjnej - Dane są szyfrowane w aplikacji lub kliencie uzyskującym dostęp do platformy.
- Szyfrowanie bazy danych - Dane są szyfrowane wykorzystując mechanizmy wbudowane I wspierane przez platformę bazodanową
- Proxy encryption: Dane przechodzą przez szyfrujące proxy zanim trafią do platformy

- Instance-managed encryption (TrueCrypt, dm-crypt Linuxa)
- Externally-managed encryption (HSM, SecaaS, Serwer)

- Szyfrowanie po stronie klienta (client-side encryption)
- Szyfrowanie po stronie serwera (server-side encryption)

ZAUFANA TRZECIA STRONA.PL

Szyfrowanie podczas przesyłu

aruba CLOUD

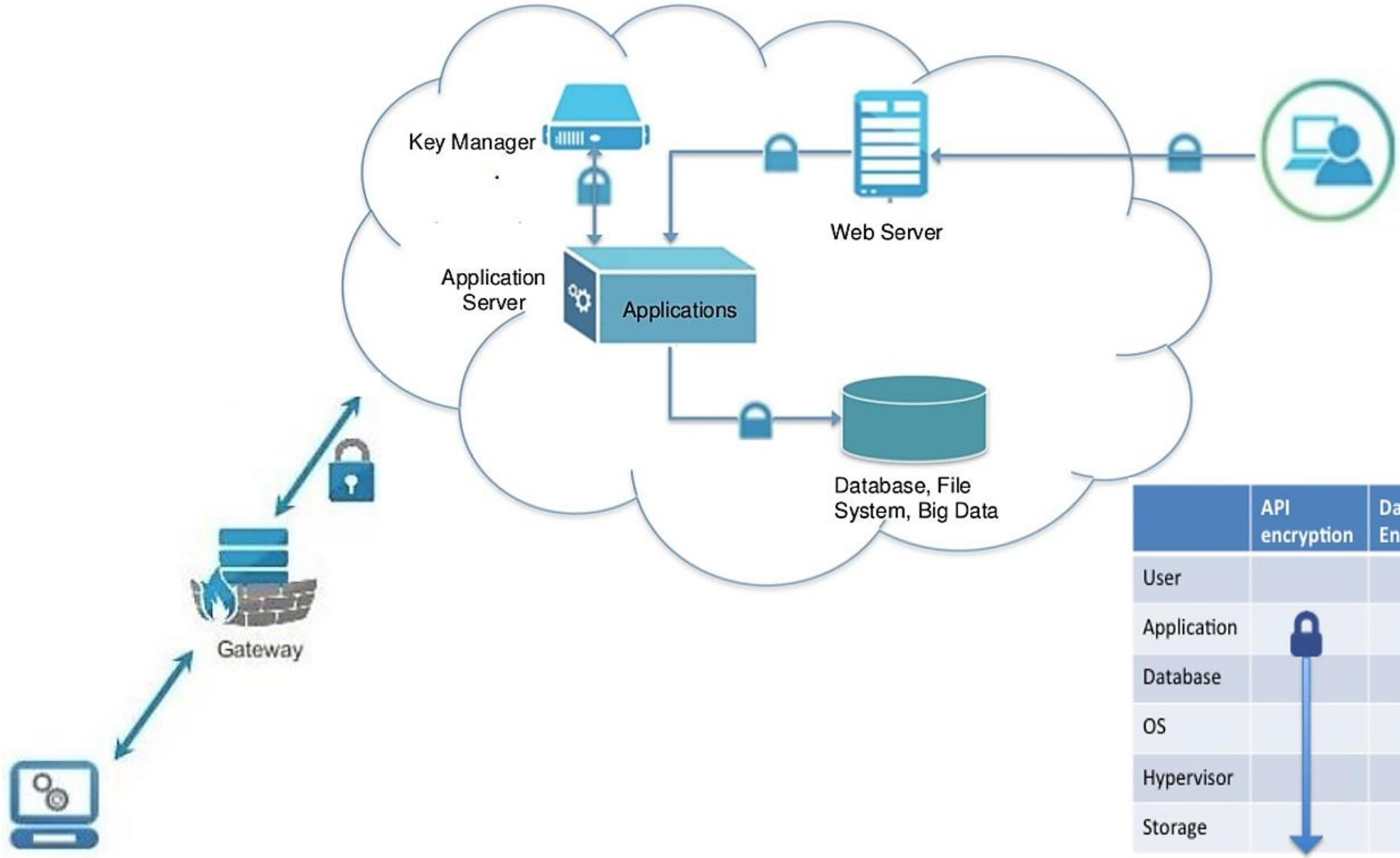
End to End encryption

IPsec

ZAUFANA TRZECIA STRONA.PL

Szyfrowanie podczas przesyłu

aruba CLOUD



	API encryption	Database Encryption	File Encryption	Storage Encryption	Gateway Encryption
User					
Application					
Database					
OS					
Hypervisor					
Storage					

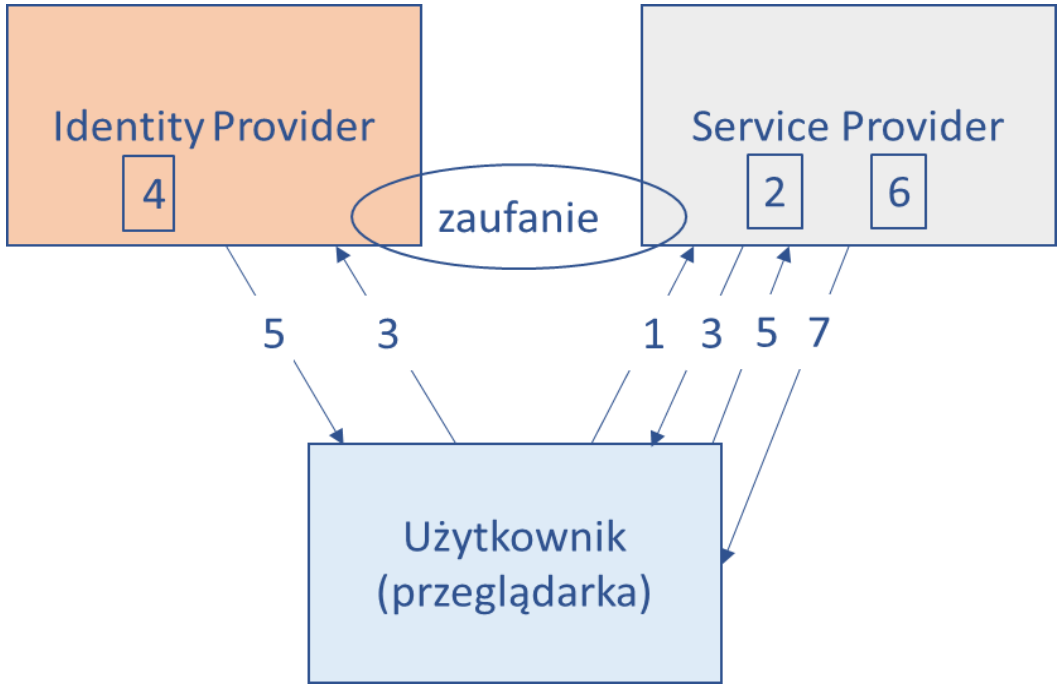
ZAUFANA TRZECIA STRONA.PL

Szyfrowanie

aruba CLOUD

Federated Identity (FIM)

- Model, w którym podmiot może korzystać z wielu usług dostarczanych przez różnych dostawców przy użyciu tych samych danych uwierzytelniających.
- W tym podejściu tożsamość podmiotu jest potwierdzana przez zaufaną stronę (Identity provider), która może być wewnętrzna jak i zewnętrzna.

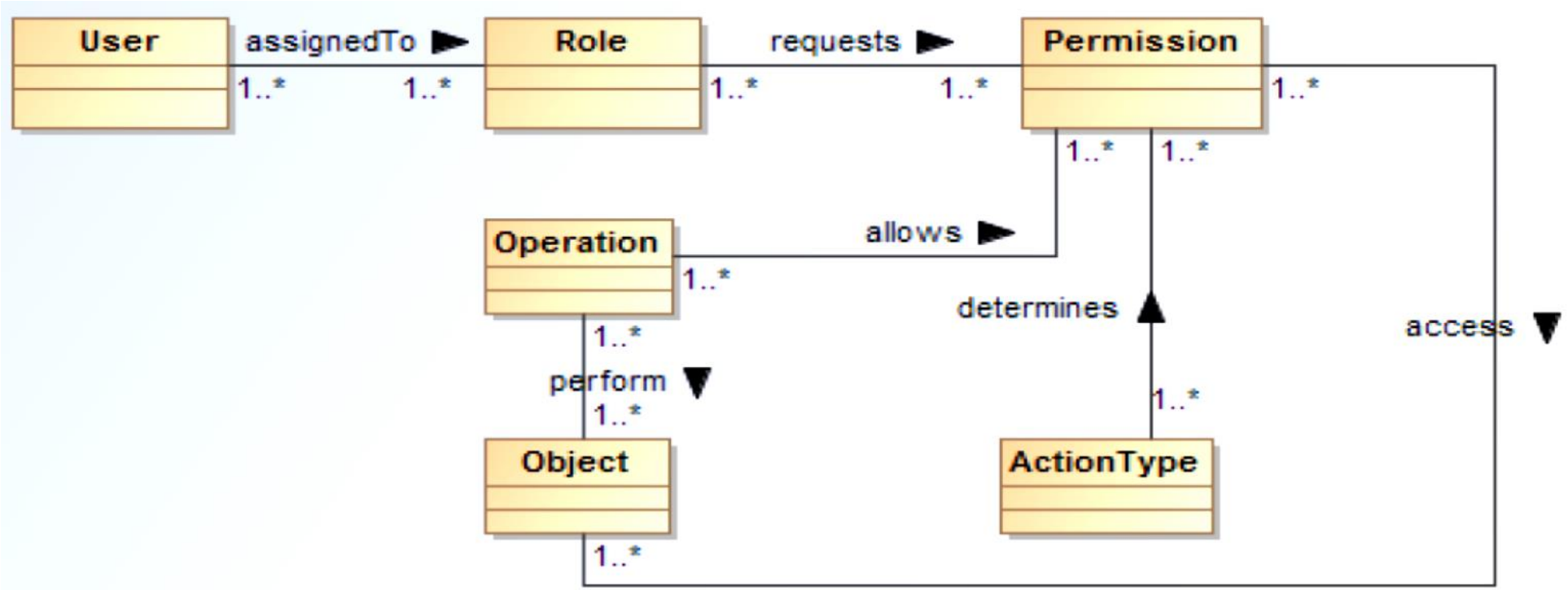


1. Użytkownik chce uzyskać dostęp do serwisu. Użytkownik może się zalogować używając danych z zaufanego serwisu pełniącego rolę Identity Provider (IdP) np. inny serwis bankowy
2. Użytkownik wybiera logowanie przy użyciu danych IdP. Service Provider (SP) generuje żądanie potwierdzenia tożsamości do Identity Provider (IdP)
3. Usługa przekierowuje użytkownika do IdP, w tym przypadku do serwisu bankowego
4. IdP uwierzytelnia użytkownika (na podstawie wprowadzonych danych uwierzytelniających lub session cookies)
5. IdP wysyła poświadczenie tożsamości do przeglądarki użytkownika, które jest przekierowane do usługi.
6. SP (Pinterest) weryfikuje potwierdzenie tożsamości.
7. Użytkownik Marcin uzyskuje dostęp do serwisu.

Kontrola dostępu - modele

RBAC - (Role based access control)

- Kontrola dostępu oparta na rolach zakłada przypisanie podmiotom odpowiednich ról, które przekładają się na poszczególne uprawnienia do wykonywania operacji w systemie.
- Podmiot może pełnić wiele ról, ale może wykorzystać uprawnienia jedynie w ramach roli, którą pełni aktualnie. Są one przydzielane ze względu na jego przynależność do roli, a nie tożsamość.
- Powiązanie uprawnień pracownika do funkcji, jaką pełnią.

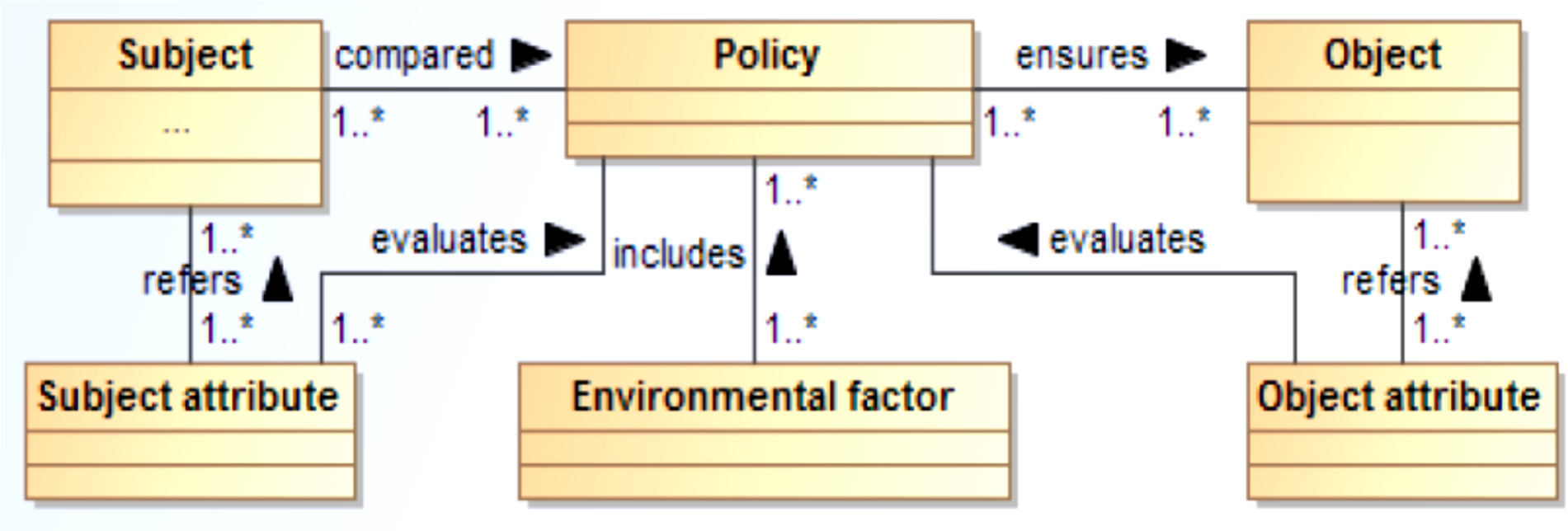


RBAC model –źródło „ Guide to Attribute Based Access Control (ABAC) Definition and Considerations”

Kontrola dostępu - modele

ABAC - (attribute-based access control)

- Dodatkowo określa kiedy, gdzie, dlaczego i jak dostęp powinien być nadany
- Polega on na nadaniu użytkownikowi zestawu atrybutów, które są cechami dla :
  - podmiotu, którym może być użytkownik, funkcja, rola czy posiadany certyfikat
  - obiektu np. urządzenie, plik, rekord, tablica, proces, program, sieć czy domena
  - warunków środowiskowych (environment conditions) stanowiących operacyjny lub sytuacyjny kontekst, w którym następuje żądanie dostępu. Mogą obejmować atrybuty związane z czasem (godziny, dni tygodnia) , geolokalizacją lub przynależnością do sieci lub domeny.
- Obiekt określa, jakie atrybuty musi posiadać podmiot łącznie z warunkami środowiskowymi, aby uzyskać do niego dostęp.

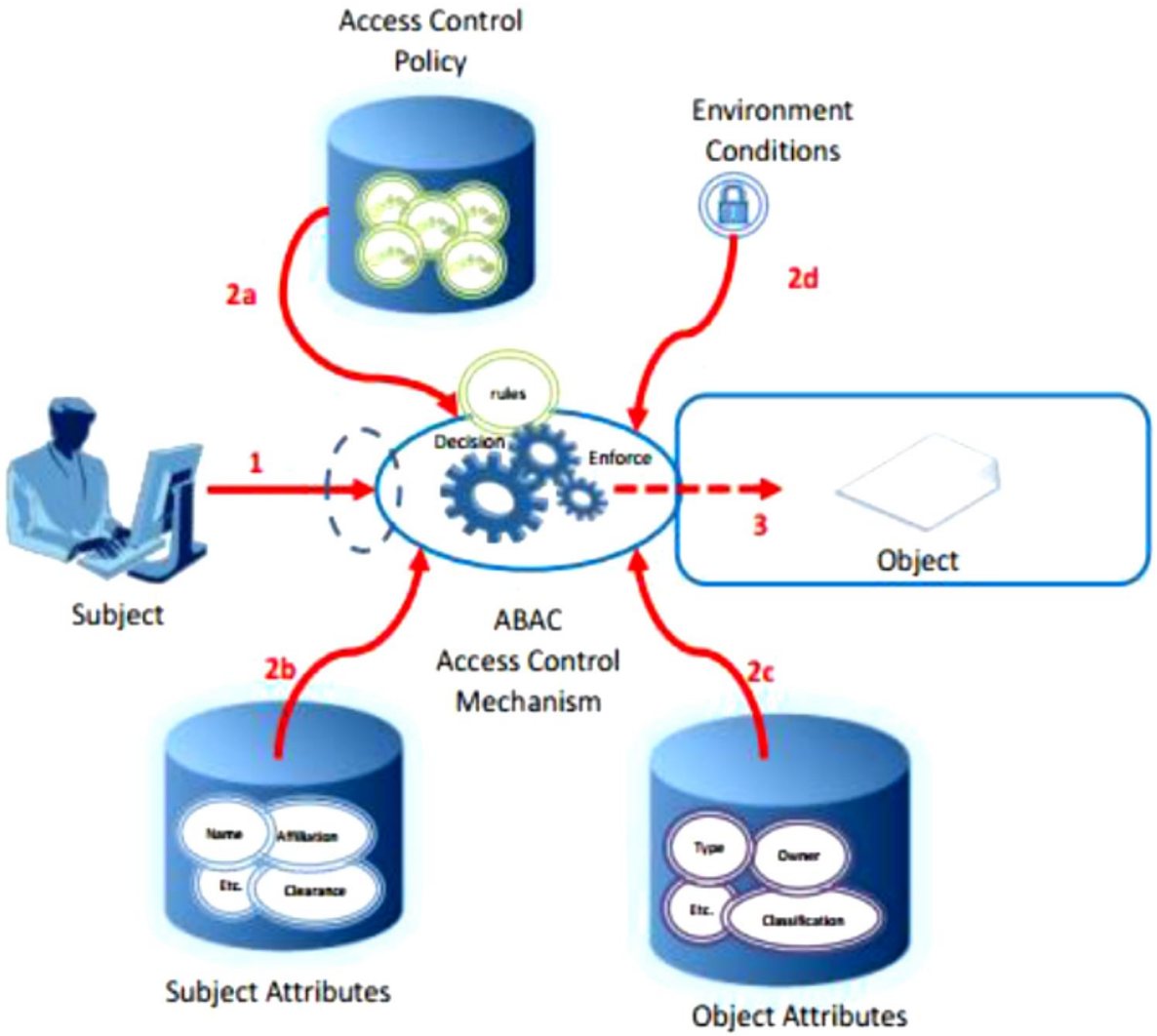


ABAC model –źródło „ Guide to Attribute Based Access Control (ABAC) Definition and Considerations”

ZAUFANA TRZECIA STRONA.PL

Kontrola dostępu - modele

aruba CLOUD



1. Podmiot chce uzyskać dostęp do obiektu
2. Mechanizm kontroli dostępu analizuje:
a. Reguły – ograniczenia dostępu. W wyniku analizy zwracana jest wartość true lub false
b. Atrybuty podmiotu
c. Atrybuty obiektu
d. Warunki środowiskowe (opcjonalnie)
3. W przypadku pozytywnej autoryzacji podmiot uzyskuje dostęp do obiektu.

Przykład: Pielęgniarka (1) z oddziału ortopedii (2b) może uzyskać dostęp w trybie do odczytu (2a) do danych aktualnych pacjentów z oddziału ortopedii (2c) w szpitalu warszawskim w trakcie swojej zmiany (2d)

ABAC model –źródło „ Guide to Attribute Based Access Control (ABAC) Definition and Considerations”

ZAUFANA TRZECIA STRONA.PL

Kontrola dostępu - modele

aruba CLOUD

Przy wyborze odpowiedniego dla używanych przez siebie rozwiązań należy wziąć pod uwagę wiele czynników m.in.:

Uwzględnienie niejednorodnej specyfiki chmury i wsparcie interoperacyjności – usługi w modelu cloud computing wykorzystują różne technologie w zakresie oprogramowania i sprzętu. Przy projektowaniu systemu kontroli dostępu należy wziąć pod uwagę jego integrację i kompatybilność z wieloma rozwiązaniami i standardami.

Złożoność rozwiązania i czas reakcji – jedna z cech chmury polegająca na szerokim, zdalnym dostępie do usług mogących znajdować się w dowolnym obszarze geograficznym. Część obecnie stosowanych modeli kontroli dostępu zapewnia wysoki poziom bezpieczeństwa okupiony jednak użyciem skomplikowanych algorytmów powodujących spowolnienie usługi.

Skalowalność – kolejna z cech usług chmurowych, która powinna być również uwzględniona w kontekście kontroli dostępu. Rozwiązanie powinno w elastyczny sposób dostosowywać się do wzrostu liczby użytkowników i polityk i umożliwiać proste zarządzanie.

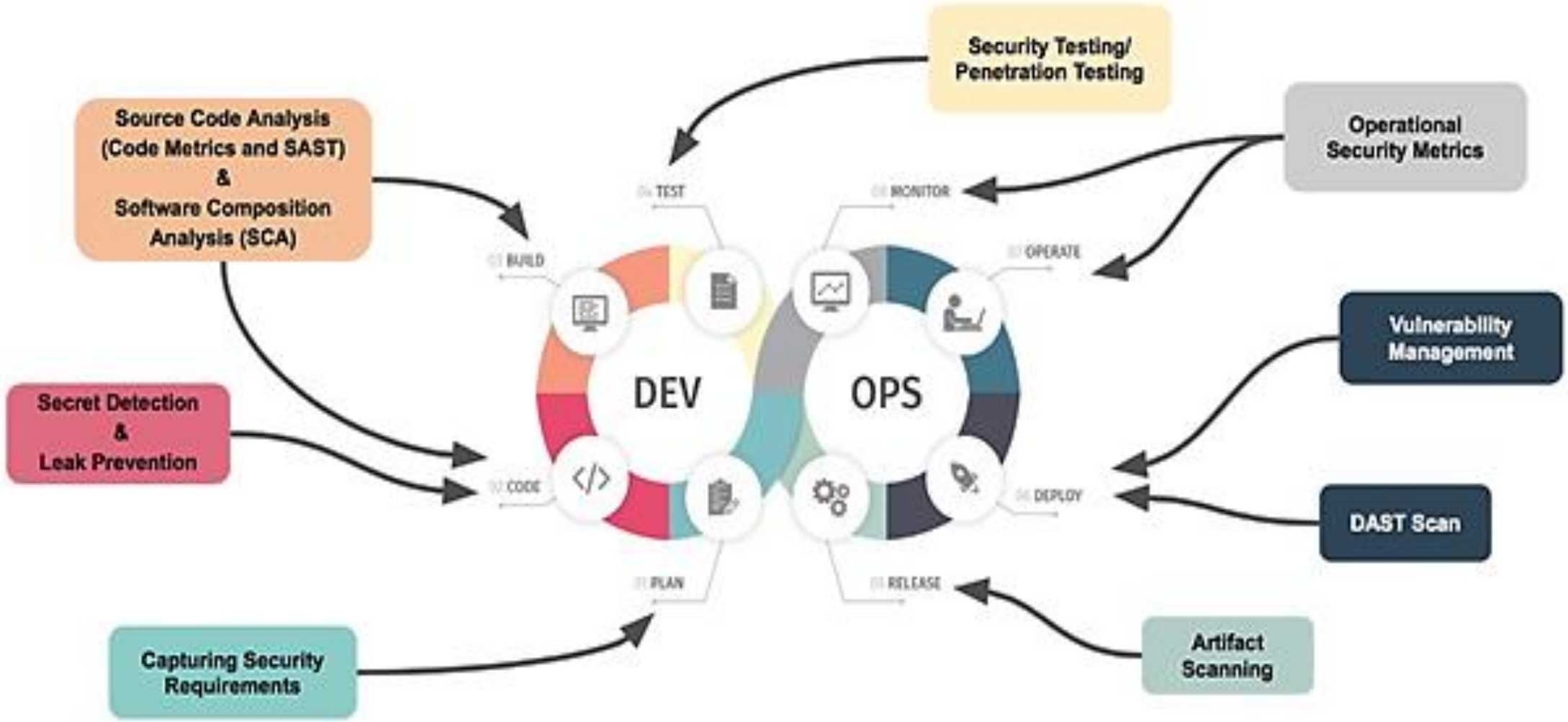
Kategoria/model	RBAC*	ABAC
Łatwość użycia	Wysoka	Średnia
Efektywność	Wysoka	Średnia
Elastyczność/ Skalowalność	Średnia	Wysoka
Bezpieczeństwo	Średnie	Wysokie
Szczegółowość dostępu (Fine grained)	Niska	Wysoka
Odpowiednia dla dynamicznych i rozproszonych środowisk	Nie	Tak

ZAUFANA TRZECIA STRONA.PL

SDLC

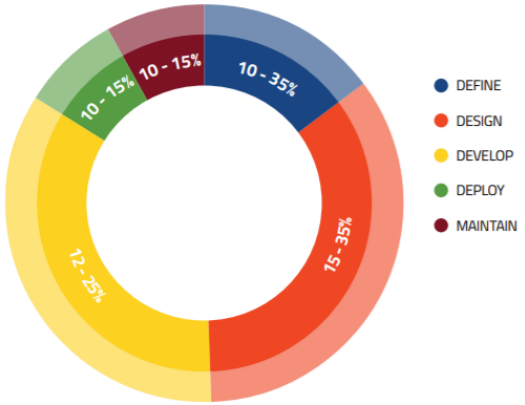
aruba CLOUD

DevOps (DevSecOps)

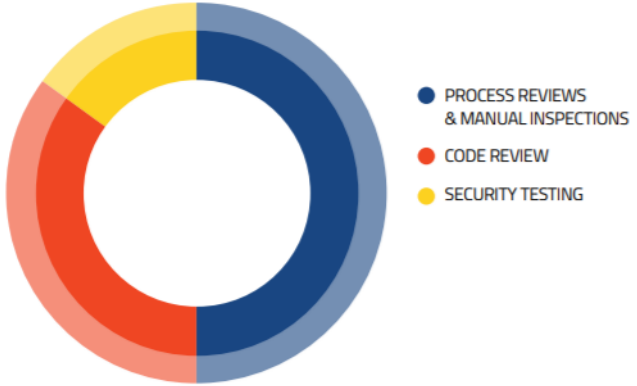


SDLC

- Zbuduj kulturę bezpieczeństwa i uczyń je stałym elementom cyklu SDLC na każdym z jego etapów.
- Testuj wcześnie i często, ale adekwatnie do potrzeb.
- Pamiętaj o współdzielonej odpowiedzialności (dostawca-odbiorca) poszczególnych warstwach stosu SPI. Uwzględnij ten aspekt przy modelowaniu zagrożeń i projektowaniu testów oraz monitorowania. Nie wszystko w chmurze jest możliwe i widoczne.
- Duży nacisk na bezpieczeństwo swoich rozwiązań
- Dodatkowe narzędzia, które łatwo można wkomponować w cykl rozwoju.
- Skalowalność, elastyczność i łatwa możliwość korzystania z mikroserwisów oraz tworzenia odseparowanych środowisk.



Rys.1 Proporcje testów na fazy cyklu (OWASP Testing Guide ver.4)



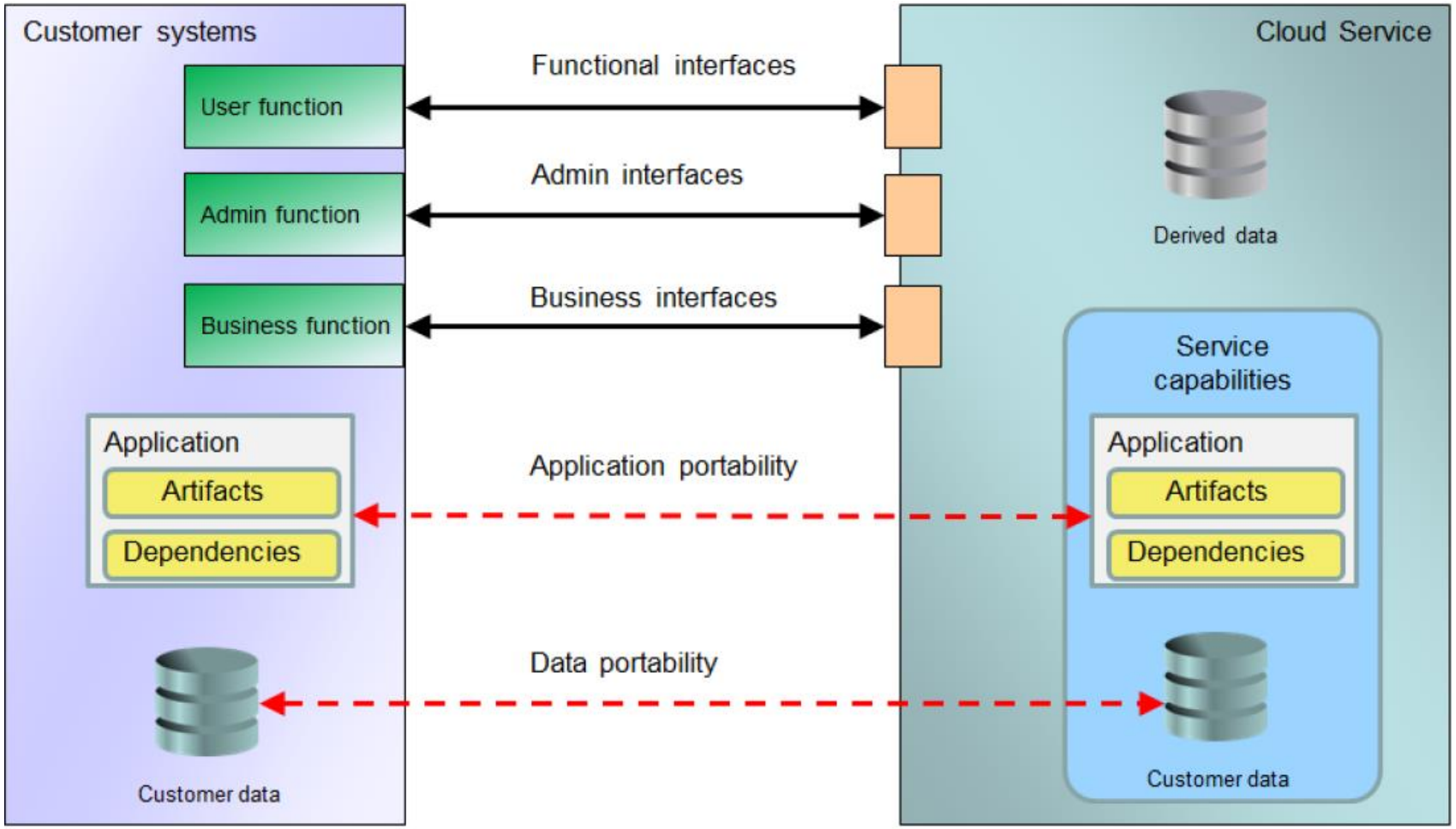
Rys.2 Proporcje testów ze względu na techniki

- Spełnienie wielu wymagań dotyczących zgodności z wieloma regulacjami.
- Jednolite interfejsy, API, narzędzia do orkiestracji i zarządzania infrastrukturą, platformą i aplikacjami, umożliwiają uzyskanie szerszego obrazu i lepszej komunikacji między zespołami DevOps

ZAUFANA TRZECIA STRONA.PL

Interoperacyjność i przenaszalność

aruba CLOUD

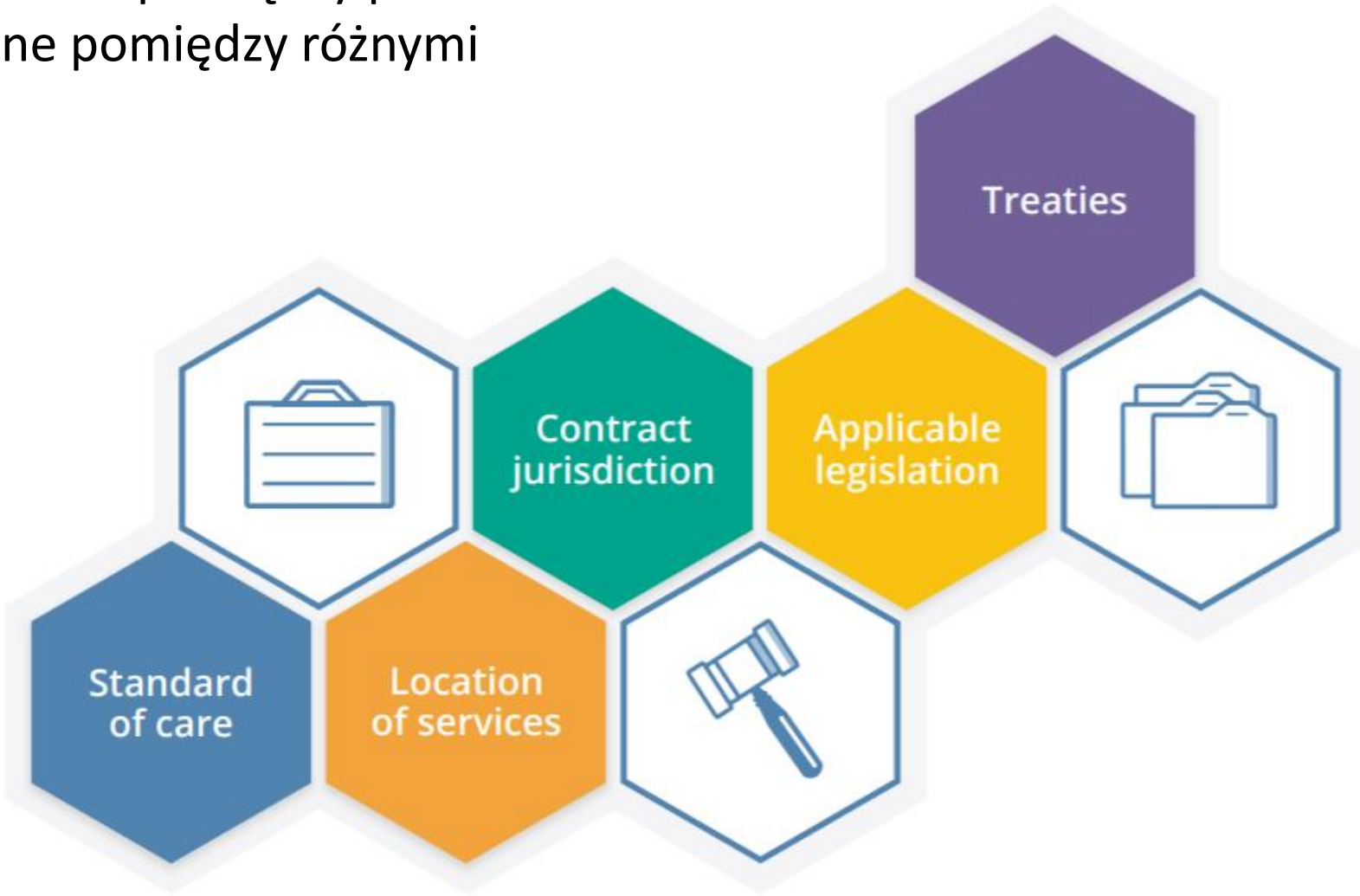


ZAUFANA TRZECIA STRONA.PL

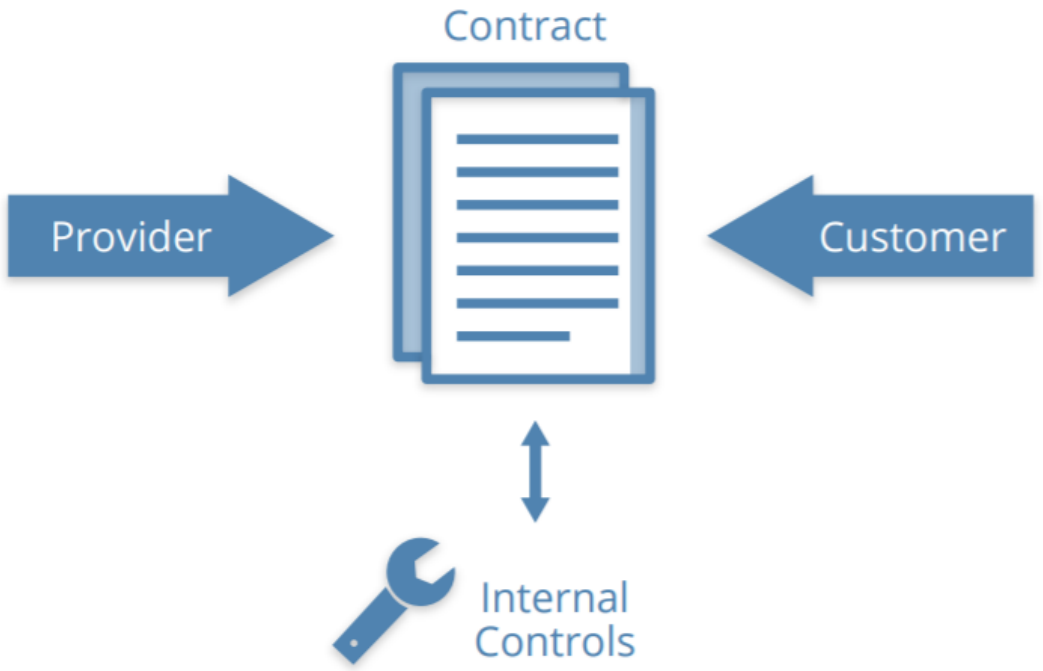
Kwestie prawne

aruba CLOUD

- Lokalizacja dostawcy, danych, serwerów
- Jurysdykcja, której podlega umowa pomiędzy podmiotami
- Traktaty i inne regulacje prawne pomiędzy różnymi lokalizacjami



Zapisy umowne



- Opis usługi
- Role i odpowiedzialności
- Zarządzanie usługą
- Dostępność usługi
- Zarządzanie ciągłością i incydentami

- Gwarancje
- Kary
- Prawo do audytu
- Płatności
- Zakończenie usług

- Zarządzanie danymi
- Zabezpieczenie danych
- Klauzule poufności
- Własność danych
- Retencja danych

- Ograniczenia odpowiedzialności
- Własność intelektualna
- Jurysdykcja
- Powierzenie przetwarzania danych osobowych

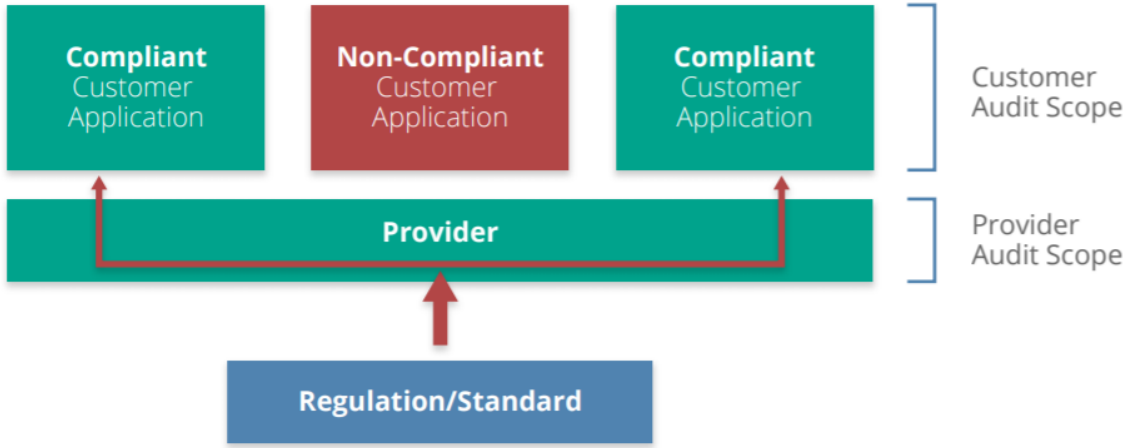
ISO/IEC 19086-1:2016 Information technology — Cloud computing — Service level agreement (SLA) framework

ZAUFANA TRZECIA STRONA.PL

Zapewnienie zgodności

aruba CLOUD

- Większe poleganie na zewnętrznych ocenach/audytach (kodeksy postępowania, certyfikaty, raporty)
- Poświadczenia potwierdzają zgodność dostawcy, nie zapewniają zgodności odbiorcy
- Współdzielona odpowiedzialność za wdrożenie wymagań, ale to odbiorca finalnie jest odpowiedzialny za zapewnienia zgodności uruchamianych aplikacji.



ZAUFANA TRZECIA STRONA.PL

Audyt w chmurze

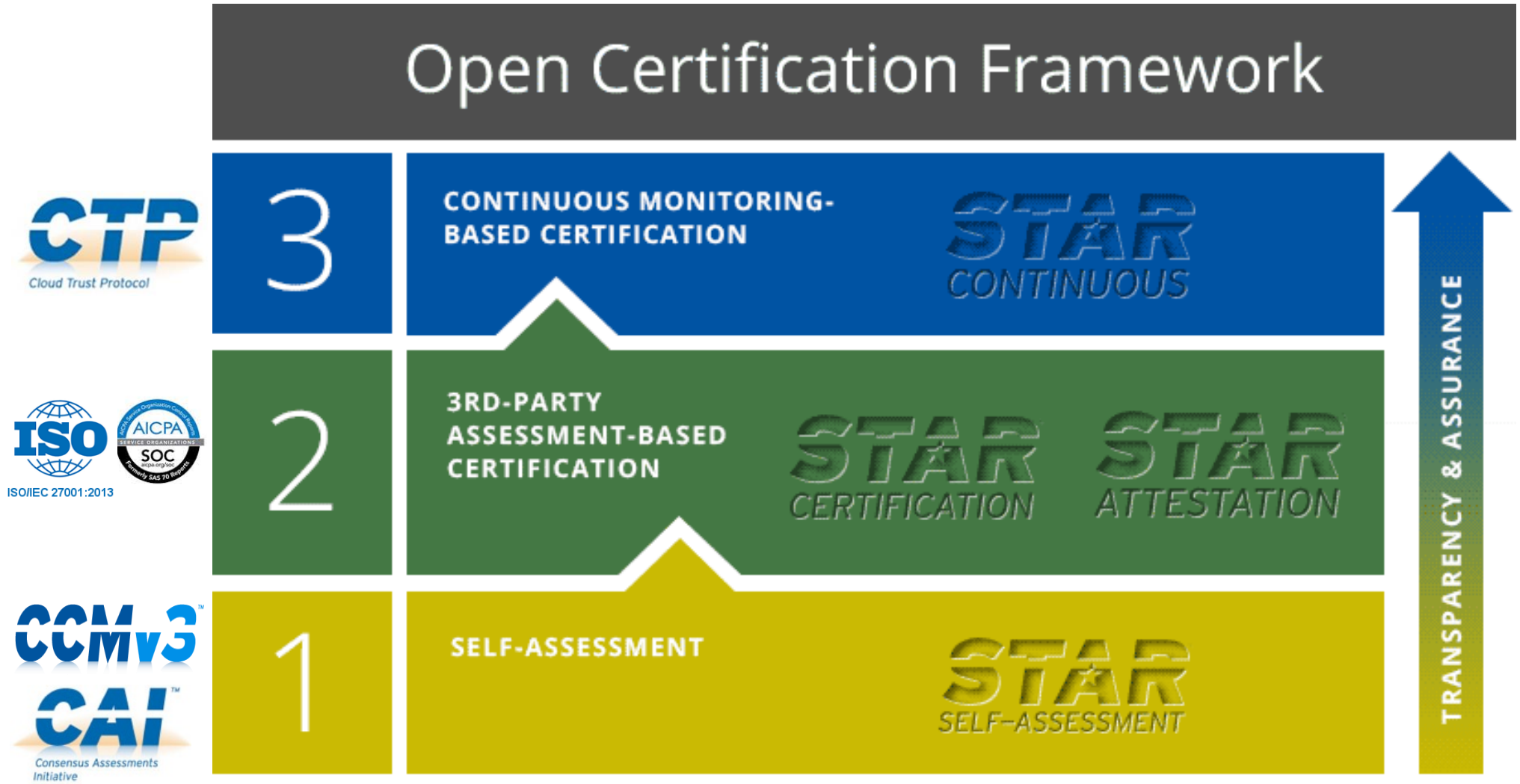
aruba CLOUD

- Cloud Computing Management Audit/Assurance Program (ISACA)
- IT Control Objectives for cloud computing (ISACA)
- Cloud Control Matrix (CCM) , Consensus Assessment Initiative (CAI), STAR
- ISO/IEC 27001:2013 certyfikat potwierdzający wdrożenie i funkcjonowanie Systemu Zarządzania Bezpieczeństwem Informacji
- ISO/IEC 27017 - zgodna z ISO/IEC 27001:2013 i uzupełniająca ISO/IEC 27002:2013, która kładzie szczególny nacisk na specyficzne zagrożenia i ryzyka związane z chmurą obliczeniową.
- ISO/IEC 27018:2014 –Praktyczne zasady ochrony informacji danych osobowych w przetwarzaniu w chmurze, uzupełniająca ISO/IEC 27002:2013 o aspekty ochrony danych osobowych w chmurze.
- Cloud Auditing Data Federation (CADF)

ZAUFANA TRZECIA STRONA.PL

STAR

aruba CLOUD



ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Q&A

Dziękuję


www.bezpiecznachmura.org.pl


bezpiecznachmura


Cloud Security Alliance Polska


biuro@bezpiecznachmura.org.pl