ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

GDPR/RODO w chmurze

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

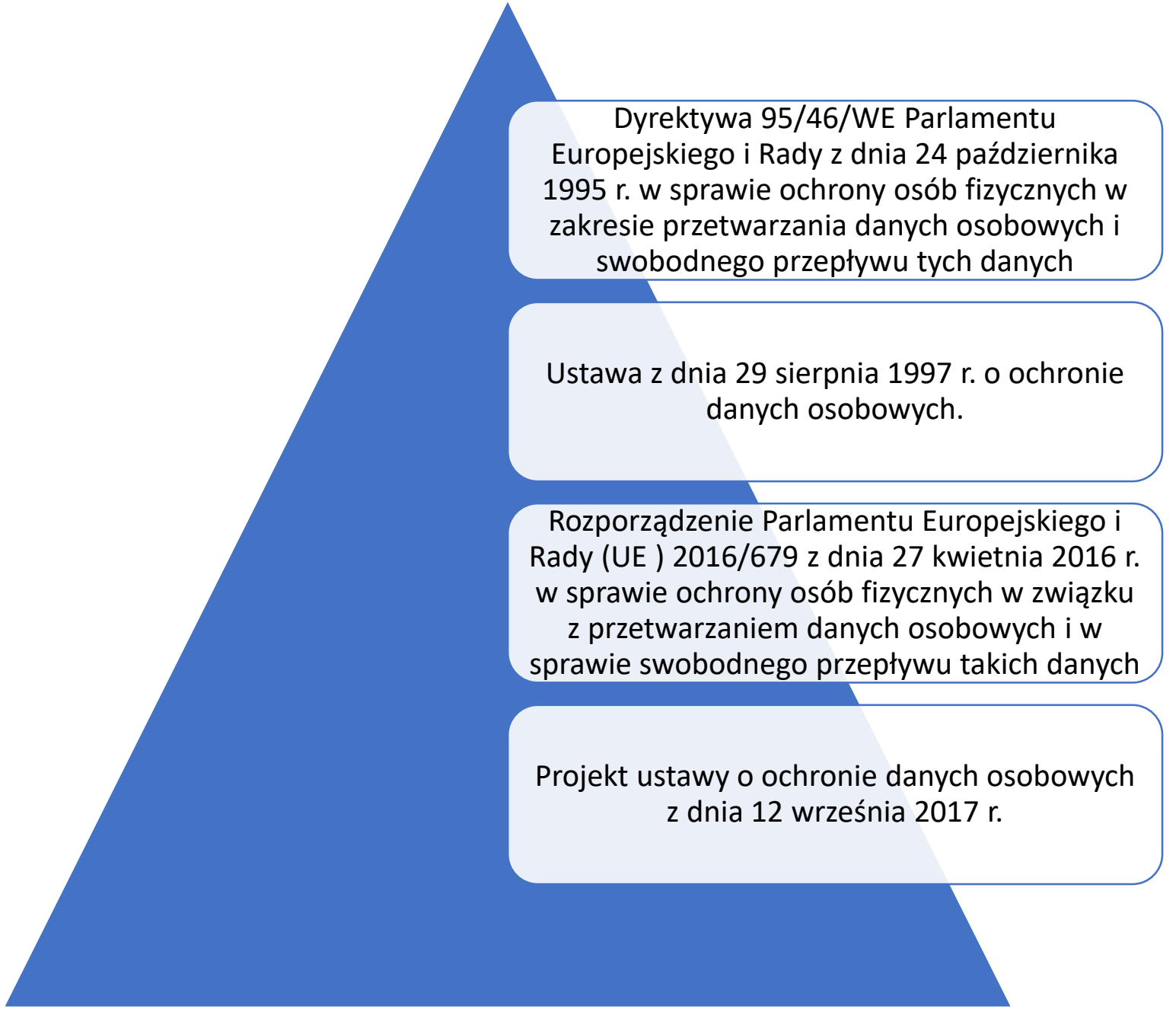
Agenda

aruba CLOUD

1. Podsumowanie zagadnień poruszanych w poprzednich artykułach
2. Wprowadzenie do RODO
3. GDPR – różnice i wpływ na usługi chmurowe
4. Podsumowanie
5. Sesja pytań od uczestników

ZAUFANA TRZECIA STRONA.PL

aruba CLOUD



GDPR

- Regulacja nie dyrektywa
- Wszelkie podmioty przetwarzające, przechowujące oraz przesyłające informacje o obywatelach UE uznane za spełniające kryteria danych osobowych
- 25 maja 2018r. – dostosowanie się do wymagań
- do 10.000.000 EUR, przedsiębiorcy do 2 % rocznego światowego obrotu
- do 20.000.000 EUR, przedsiębiorcy do 4 % rocznego światowego obrotu

http://ec.europa.eu

ZAUFANA TRZECIA STRONA.PL

Różnice

aruba CLOUD

1. Rozszerzenie definicji zbioru danych osobowych
2. Risk based approach – podejście oparte na ryzyku
3. Dodefiniowanie odpowiedzialności Administratora i Przetwarzającego
4. Prawa podmiotów

- Rozszerzony obowiązek informowania
- Prawo do zapomnienia (usuwanie i retencja)
- Prawo do przenoszenia danych

6. Wykrywanie i zgłaszanie incydentów ochrony danych osobowych
7. Privacy by design
8. Privacy by default
9. Profilowanie i marketing
10. Kodeksy postępowania i certyfikacja

ZAUFANA TRZECIA STRONA.PL

Rozszerzenie definicji DO

aruba CLOUD

- ✓ wszystkie informacje które mogą posłużyć do bezpośredniego lub pośredniego zidentyfikowania danej osoby.
- ➢ identyfikator sieciowy
- ➢ adres IP
- ➢ zmienne przechowywane w formie ciasteczek (ang. „cookies”),
- ➢ informacje powiązane z wizerunkiem (tj. zdjęcia)
- ➢ numery telefonów
- ➢ metadane profilujące zachowania i preferencje użytkowników
- ➢ dane lokalizacyjne – pozwalające określić miejsce przebywania danej osoby lub śledzić jej przemieszczanie.

ZAUFANA TRZECIA STRONA.PL

Podejście oparte na ryzyku

aruba CLOUD

- Nie jest jasno zdefiniowany sposób analizy ryzyka (ISO 27005, ISACA, CSA)
- Wysokie ryzyko naruszenia praw lub wolności osób fizycznych > Ocena skutków dla ochrony danych – (DPIA)

➢ Ewaluacja, profilowanie, zautomatyzowane podejmowanie decyzji
➢ Przetwarzanie na dużą skalę szczególnych kategorii danych osobowych
➢ Systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie
➢ Do celów DPIA–uwzględnia się przestrzeganie przez takiego administratora lub taki podmiot przetwarzający zatwierdzonych kodeksów postępowania

Administrator i Przetwarzający

Administrator:

- oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych
- wdraża odpowiednie i skuteczne środki techniczne i organizacyjne:

1) mają one zapewniać najwyższy znany i możliwy w chwili przetwarzania danych, poziom ochrony;
2) nie może być to czynność jednorazowa, środki te są w razie potrzeby poddawane przeglądom i uaktualniane;
3) dokonuje on tego, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia;
4) jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki te, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych

Administrator i Przetwarzający

Przetwarzający:

- wyznacza Inspektora Ochrony Danych Osobowych (IOD)
- przetwarza w imieniu administratora na podstawie umowy
- nie korzysta z usług innego procesora bez zgody administratora
- zapewnia wdrożenie odpowiednich środków technicznych i organizacyjnych oraz zachowanie tajemnicy
- podejmuje wszelkie środki wymagane na mocy art. 32
- pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36
- odpowiada za działania podprocesora
- umożliwia audyty i inspekcje, współpracuje z organem nadzorczym

Administrator i Przetwarzający

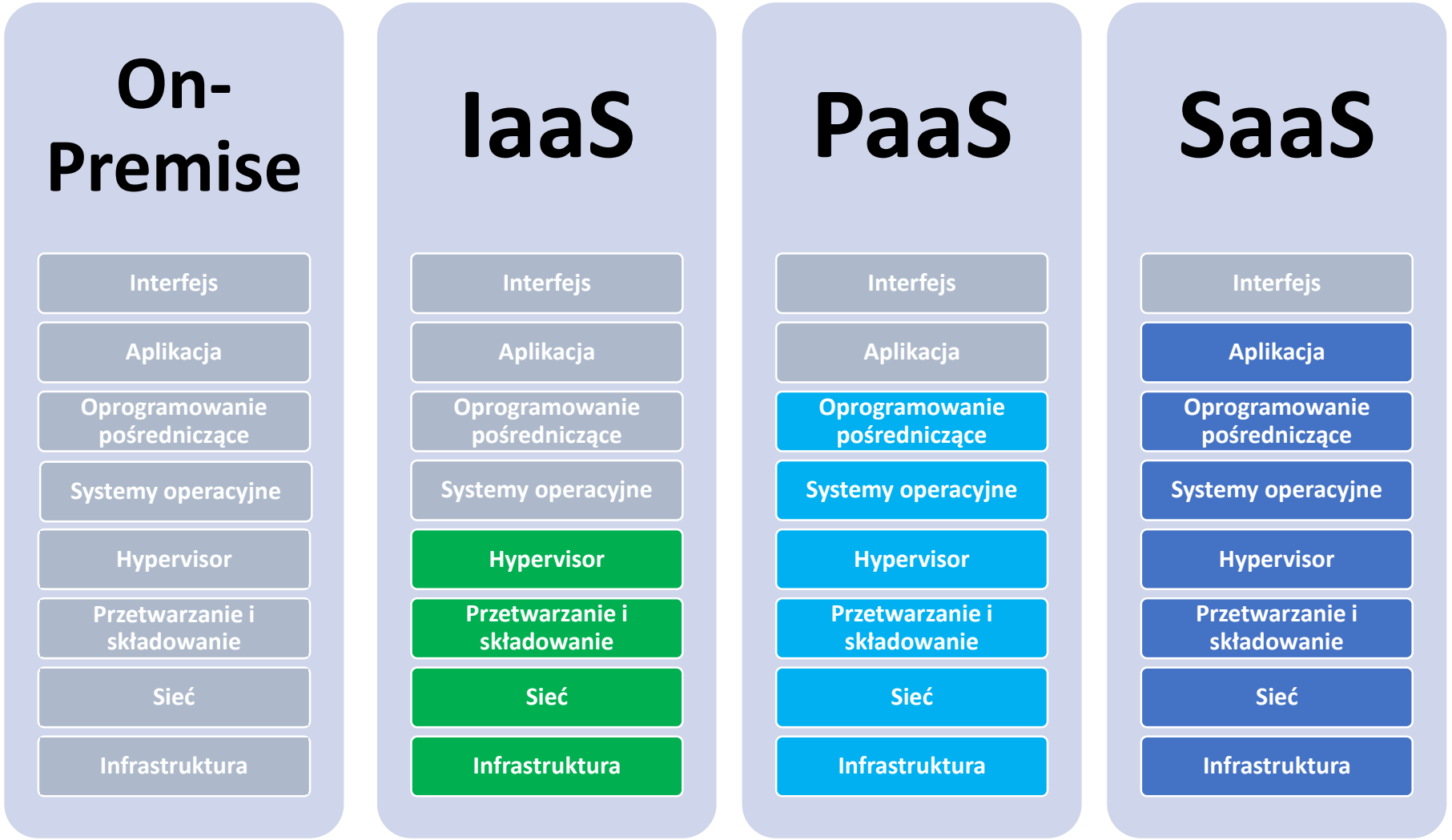
Art.82

1. Każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę.
2. Każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym niniejsze rozporządzenie. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które niniejsze rozporządzenie nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom.
3. Administrator lub podmiot przetwarzający zostają zwolnieni z odpowiedzialności wynikającej z ust. 2, jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody.

ZAUFANA TRZECIA STRONA.PL

Odpowiedzialność

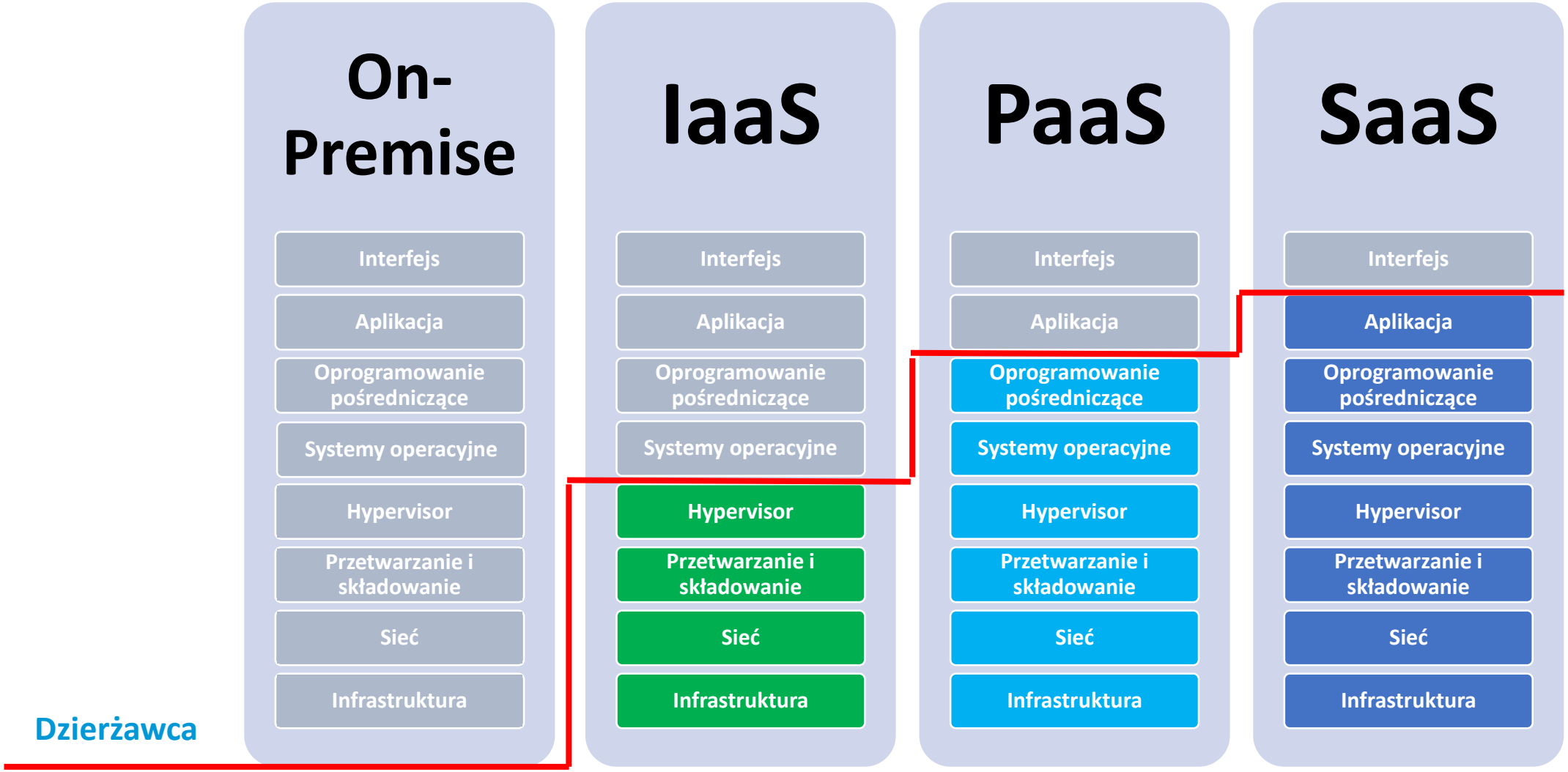
aruba CLOUD



ZAUFANA TRZECIA STRONA.PL

Odpowiedzialność

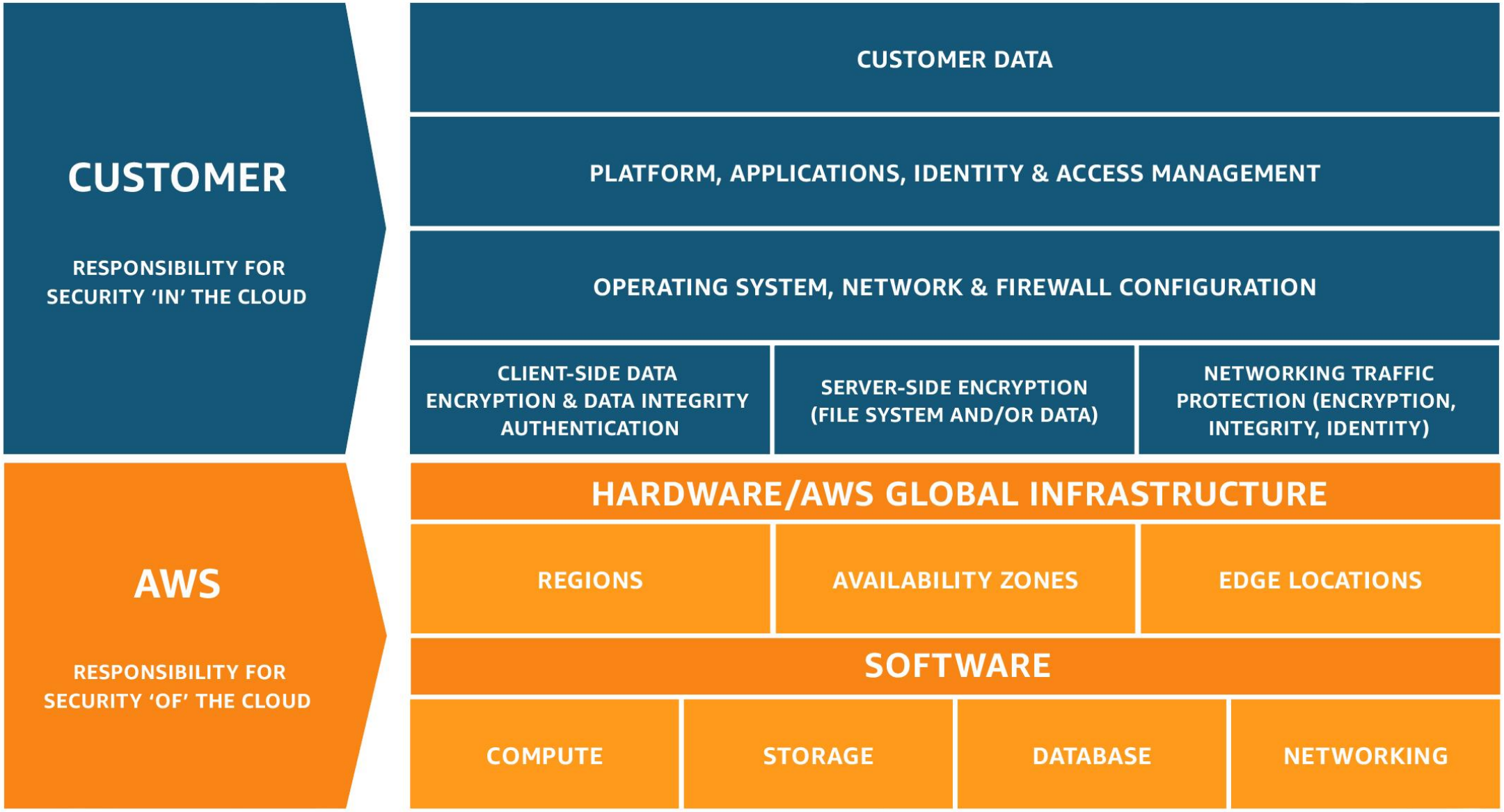
aruba CLOUD



ZAUFANA TRZECIA STRONA.PL

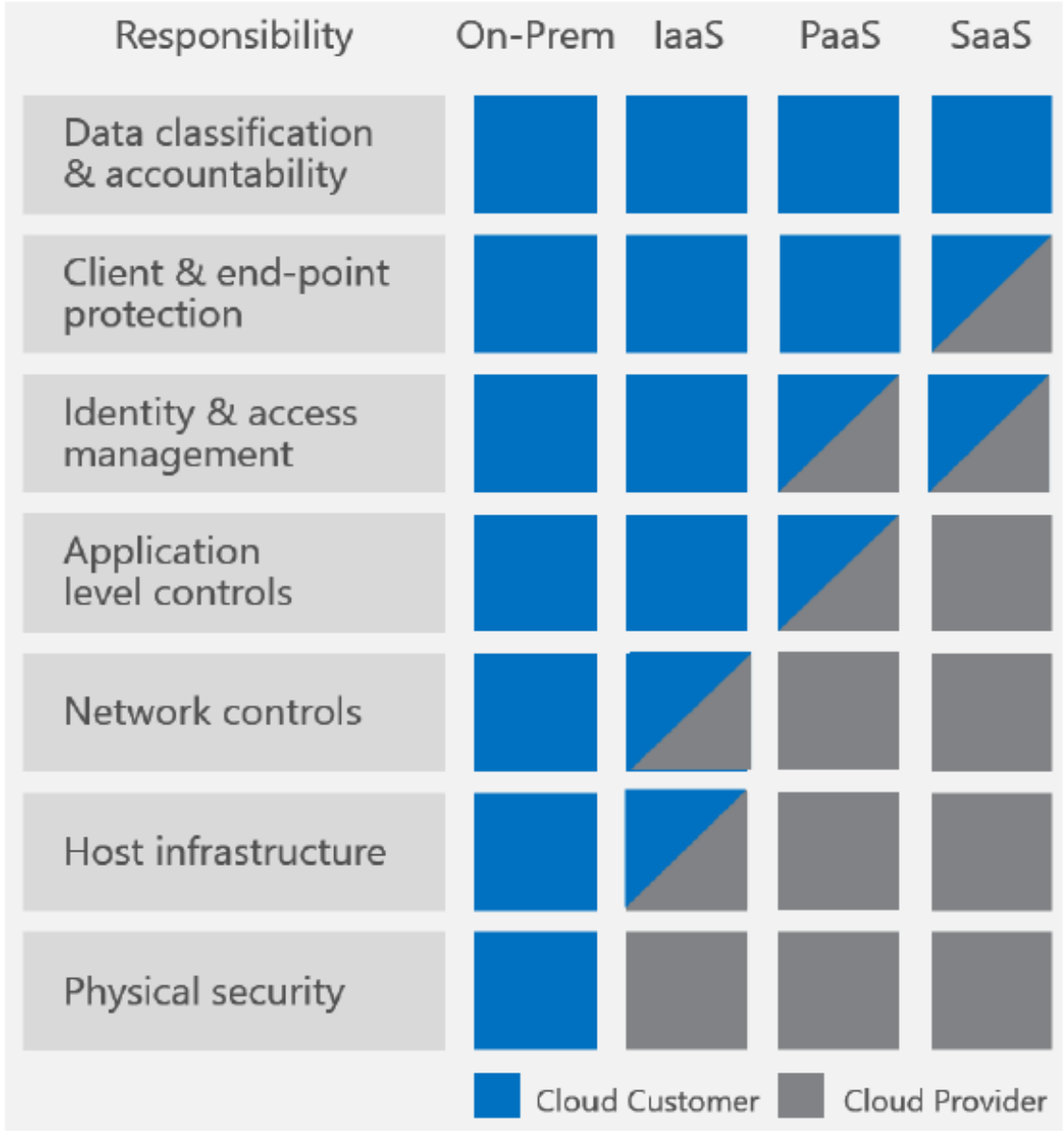
Odpowiedzialność

aruba CLOUD



ZAUFANA TRZECIA STRONA.PL

Odpowiedzialność



aruba CLOUD

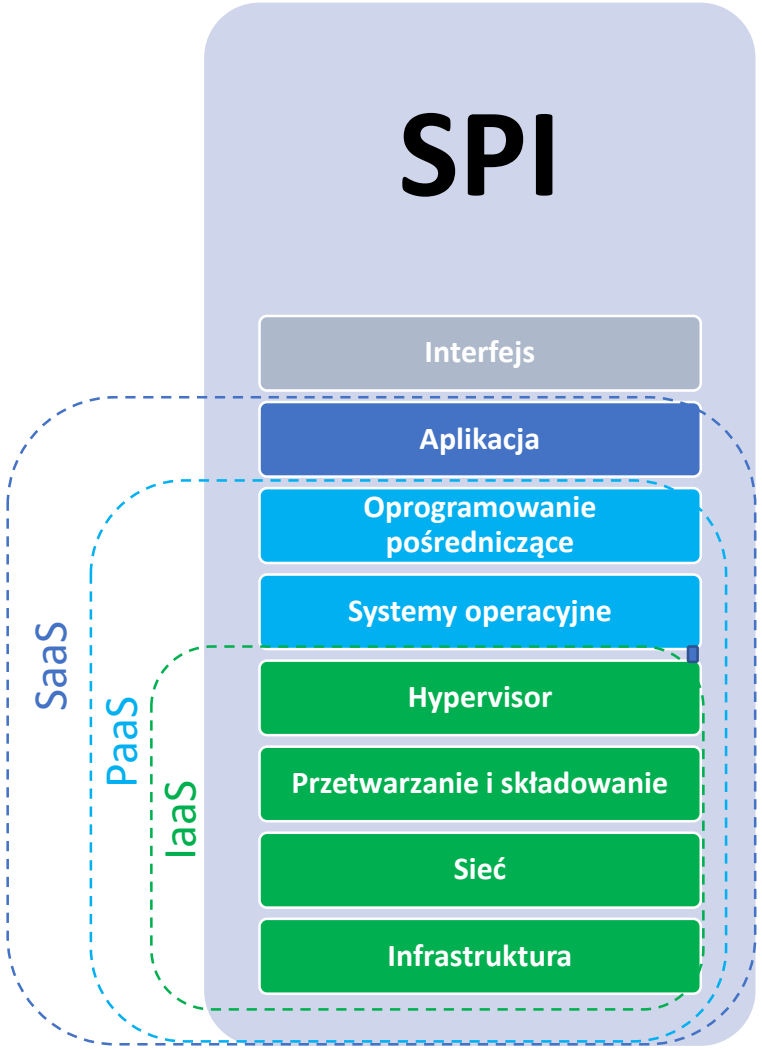
ZAUFANA TRZECIA STRONA.PL

Odpowiedzialność

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
Bezpieczeństwo fizyczne/środ.	Odbiorca	Odbiorca	Dostawca	Dostawca	Dostawca	Dostawca

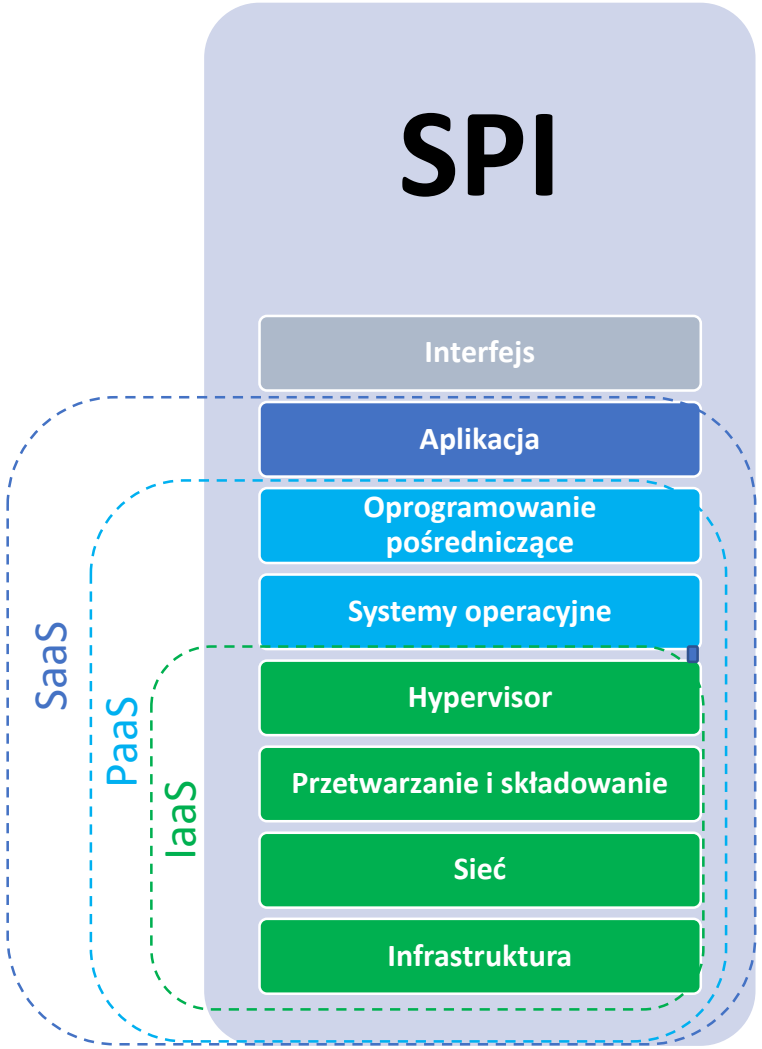
Bezpieczeństwo przetwarzania



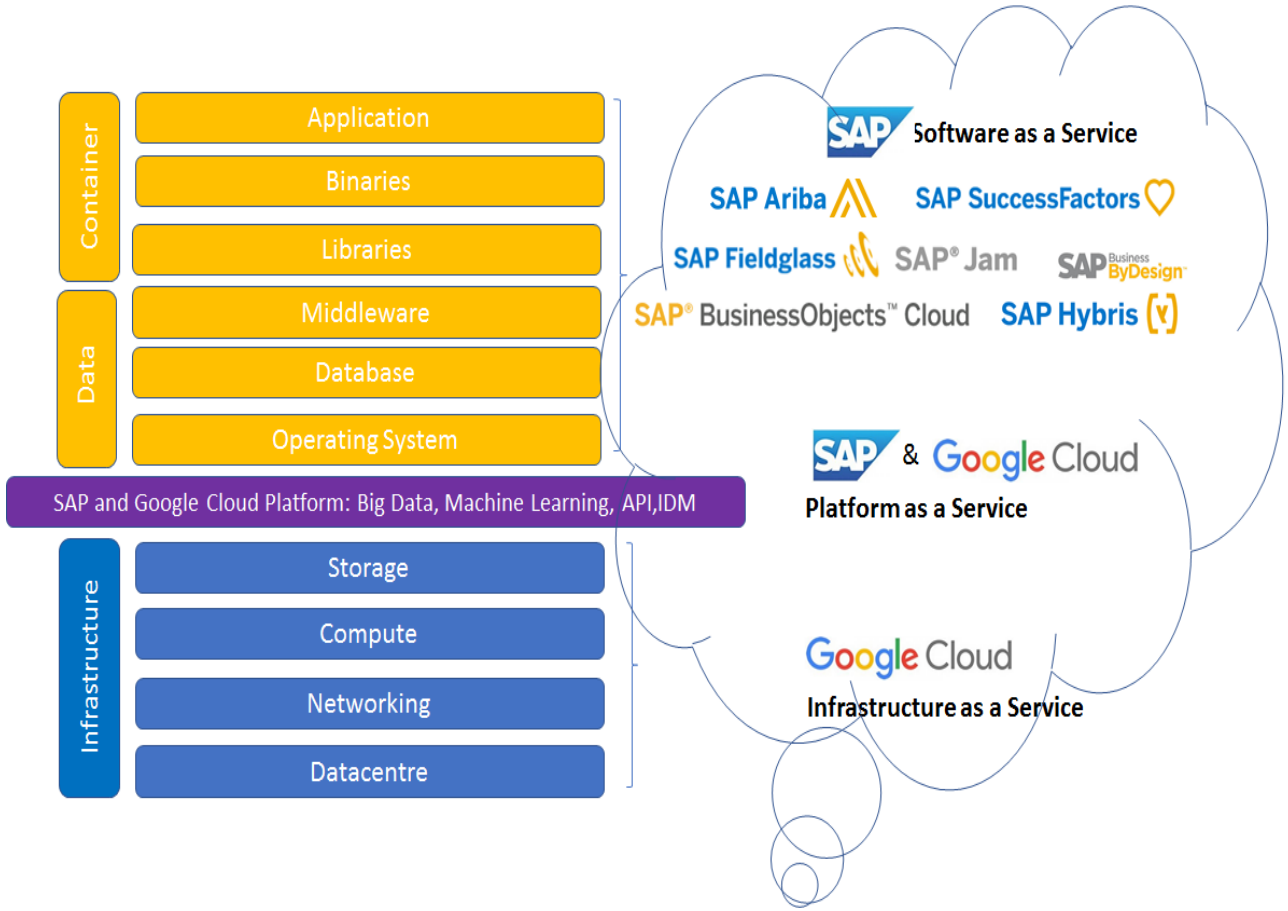
Przetwarzający podejmuje wszelkie środki wymagane na mocy art. 32:

- oparte na wynikach analizy ryzyka
- pseudonimizację i szyfrowanie danych osobowych;
- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania;
- wywiązywanie się z obowiązków można wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania lub zatwierdzonego mechanizmu certyfikacji;

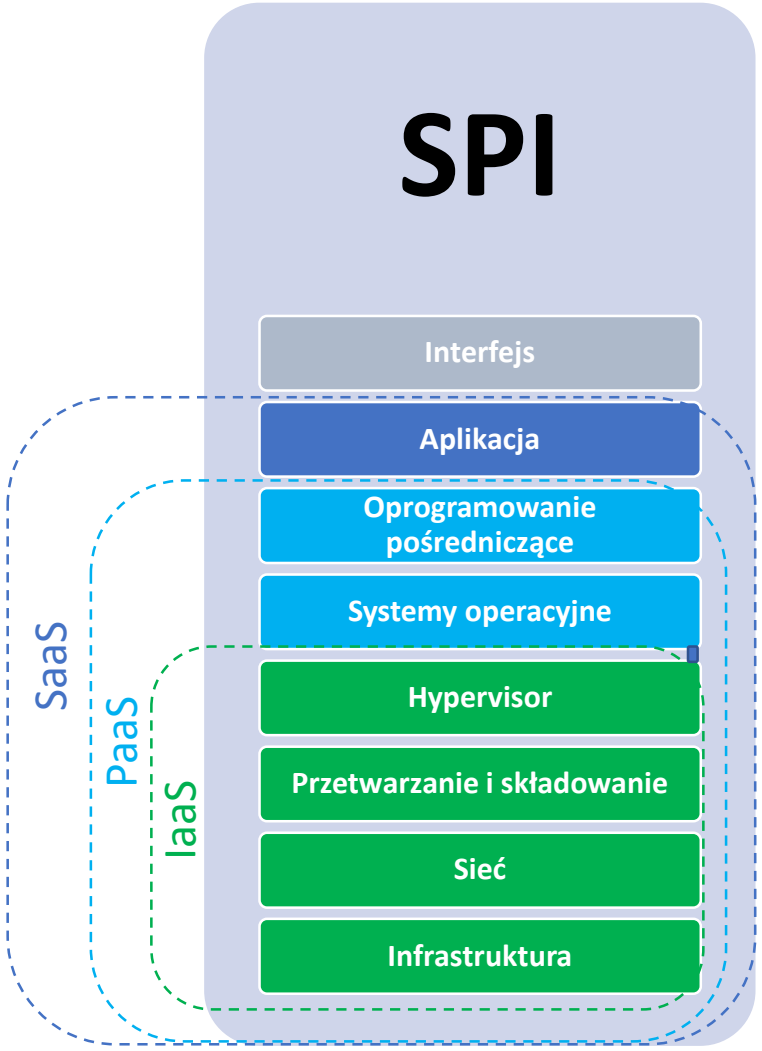
Łańcuch dostaw



- Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora.
- podejmuje wszelkie środki wymagane na mocy art. 32
- Administrator>Procesor>Podprocesor

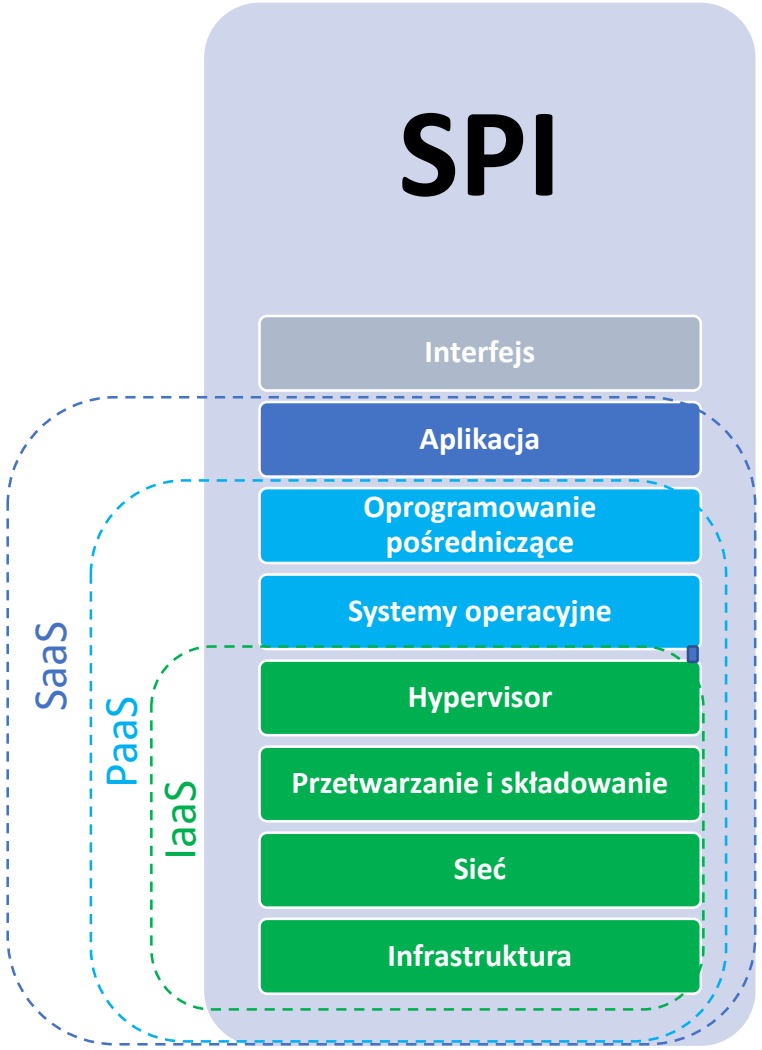


Zgłaszanie naruszenia danych



Skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych.
Administrator > Organ Nadzorczy - Nie później niż w terminie 72 godzin po stwierdzeniu naruszenia
Administrator
Administrator > Podmiot – bez zbędnej zwłoki
Procesor (Podprocesor?) >Administrator - przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych **bez zbędnej zwłoki** zgłasza je administratorowi.
Współdzierżawa – kolejność zgłoszeń

Prawa podmiotu

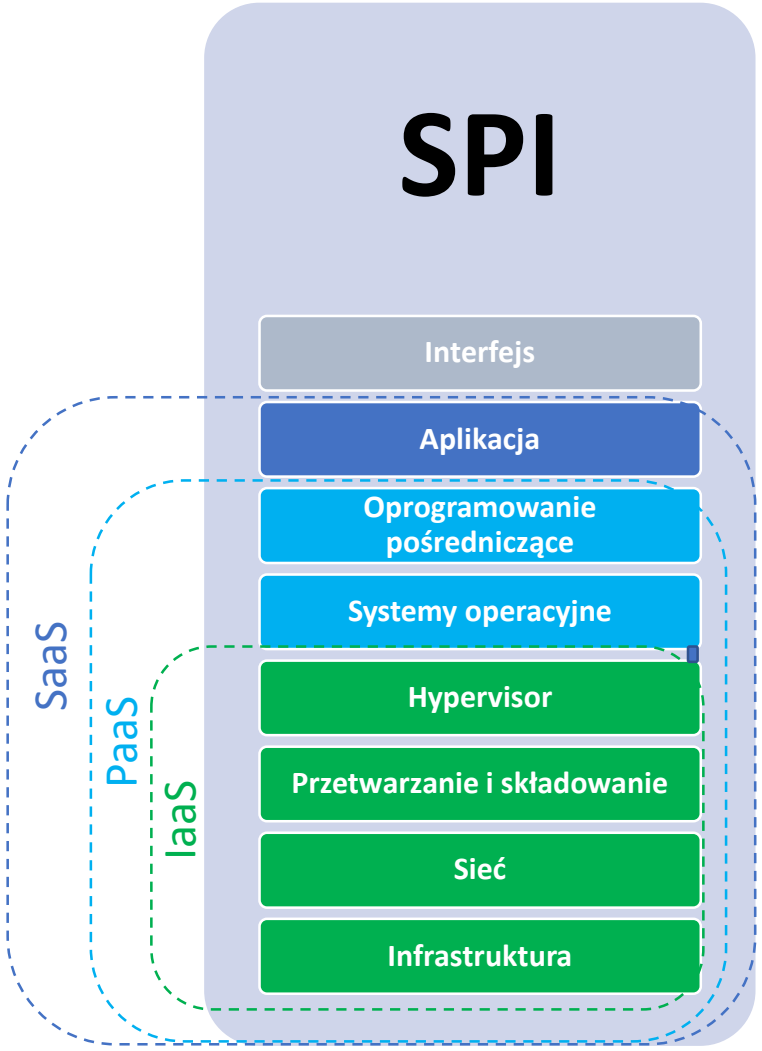


- Prawo dostępu
- Prawo do sprostowania danych
- Prawo do ograniczenia przetwarzania
- Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania
- Prawo do przenoszenia
- Prawo do usunięcia danych („prawo do bycia zapomnianym”)

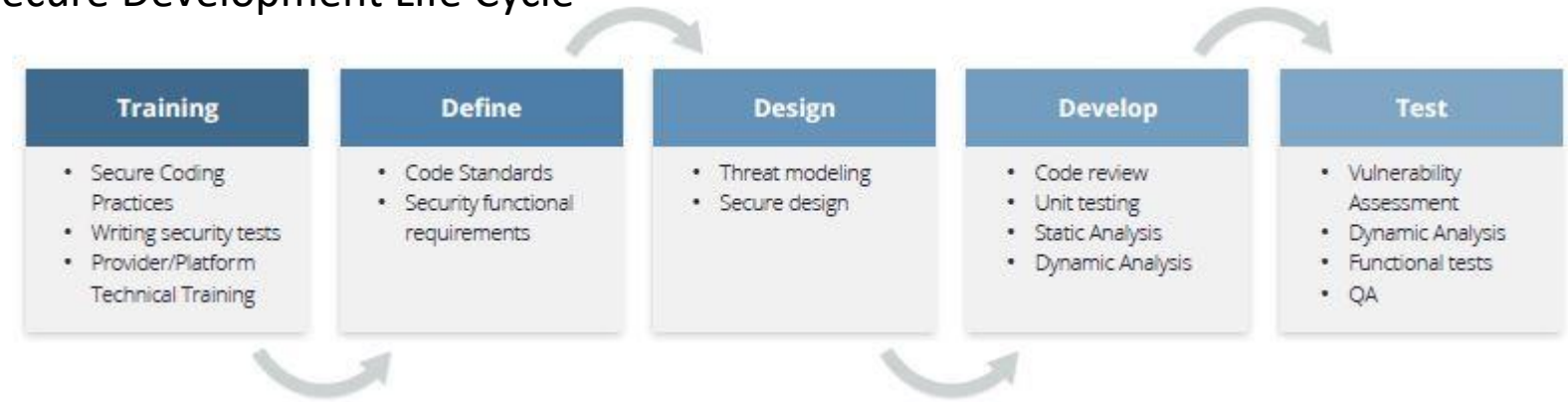
ZAUFANA TRZECIA STRONA.PL

Privacy by design

aruba CLOUD



Secure Development Life Cycle



Kodeksy postępowania i certyfikacja

ISO 27001 27002 27017 27018

EU CLOUD COC

CISPE.cloud

CSA cloud security alliance SM

ZAUFANA TRZECIA STRONA.PL

CSA Security Guidance ver.4

aruba CLOUD

Działania operacyjne

- Architektura chmury
- Nadzór i zarządzanie ryzykiem
- Prawo i informatyka śledcza
- Zgodność i audyt
- Zarządzanie informacją i ochrona danych
- Przenaszalność i interoperacyjność
- Zarządzanie ciągłością i plany awaryjne
- Centrum danych i zarządzanie operacjami
- Zarządzanie incydentami
- Bezpieczeństwo aplikacji
- Szyfrowanie i zarządzanie kluczami
- Zarządzanie własnością, tożsamością i dostępem
- Wirtualizacja
- Security as a Service

Zarządzanie w chmurze

CCM

HIPAA Health Insurance Portability and Accountability Act

enisa European Network and Information Security Agency

COBIT 5 AN ISACA® FRAMEWORK

GDPR EU General Data Protection Regulation

ISO 27001 27002 27017 27018

NIST SP 800-53 R3/R4

PCI DSS COMPLIANT

Bundesamt für Sicherheit in der Informationstechnik

IaaS	PaaS	SaaS
Public		Private
Physical	Network	Compute
Storage	Application	Data
Service/Provider		Tenant/Consumer

cloudsecurityalliance.org/guidance

ZAUFANA TRZECIA STRONA.PL

Cloud Control Matrix ver.3.0.1

aruba CLOUD

1. **AIS**: Application & Interface Security (4)
2. **AAC**: Audit Assurance & Compliance (3)
3. **BCR**: Business Continuity Management & Operational Resilience (11)
4. **CCC**: Change Control & Configuration Management (5)
5. **DSI**: Data Security & Information Lifecycle Management (7)
6. **DCS**: Datacenter Security (9)
7. **EKM**: Encryption & Key Management (4)
8. **GRM**: Governance and Risk Management (11)
9. **HRS**: Human Resources (11)
10. **IAM**: Identity & Access Management (13)
11. **IVS**: Infrastructure & Virtualization Security (13)
12. **IPY**: Interoperability & Portability (5)
13. **MOS**: Mobile Security (20)
14. **SEF**: Security Incident Management, E-Discovery & Cloud Forensics (5)
15. **STA**: Supply Chain Management, Transparency and Accountability (9)
16. **TVM**: Threat and Vulnerability Management (3)

16 domen

133 zabezpieczenia

ZAUFANA TRZECIA STRONA.PL

Cloud Control Matrix ver.3.0.1

aruba CLOUD

Application & Interface Security (AIS)

- AIS-01: Application Security
- AIS-02: Customer Access Requirements
- AIS-03: Data Integrity
- AIS-04: Data Security / Integrity

Audit Assurance & Compliance (AAC)

- AAC-01: Audit Planning
- AAC-02: Independent Audits
- AAC-03: Information System Regulatory Mapping

Business Continuity Management & Operational Resilience (BCR)

- BCR-01: Business Continuity Planning
- BCR-02: Business Continuity Testing
- BCR-03: Datacenter Utilities / Environmental Conditions
- BCR-04: Documentation
- BCR-05: Environmental Risks
- BCR-06: Equipment Location
- BCR-07: Equipment Maintenance
- BCR-08: Equipment Power Failures
- BCR-09: Impact Analysis
- BCR-10: Policy
- BCR-11: Retention Policy

Change Control & Configuration Management (CCC)

- CCC-01: New Development / Acquisition
- CCC-02: Outsourced Development
- CCC-03: Quality Testing
- CCC-04: Unauthorized Software Installations
- CCC-05: Production Changes

Data Security & Information Lifecycle Management (DSI)

- DSI-01: Classification
- DSI-02: Data Inventory / Flows
- DSI-03: eCommerce Transactions
- DSI-04: Handling / Labeling / Security Policy
- DSI-05: Non-Production Data
- DSI-06: Ownership / Stewardship
- DSI-07: Secure Disposal

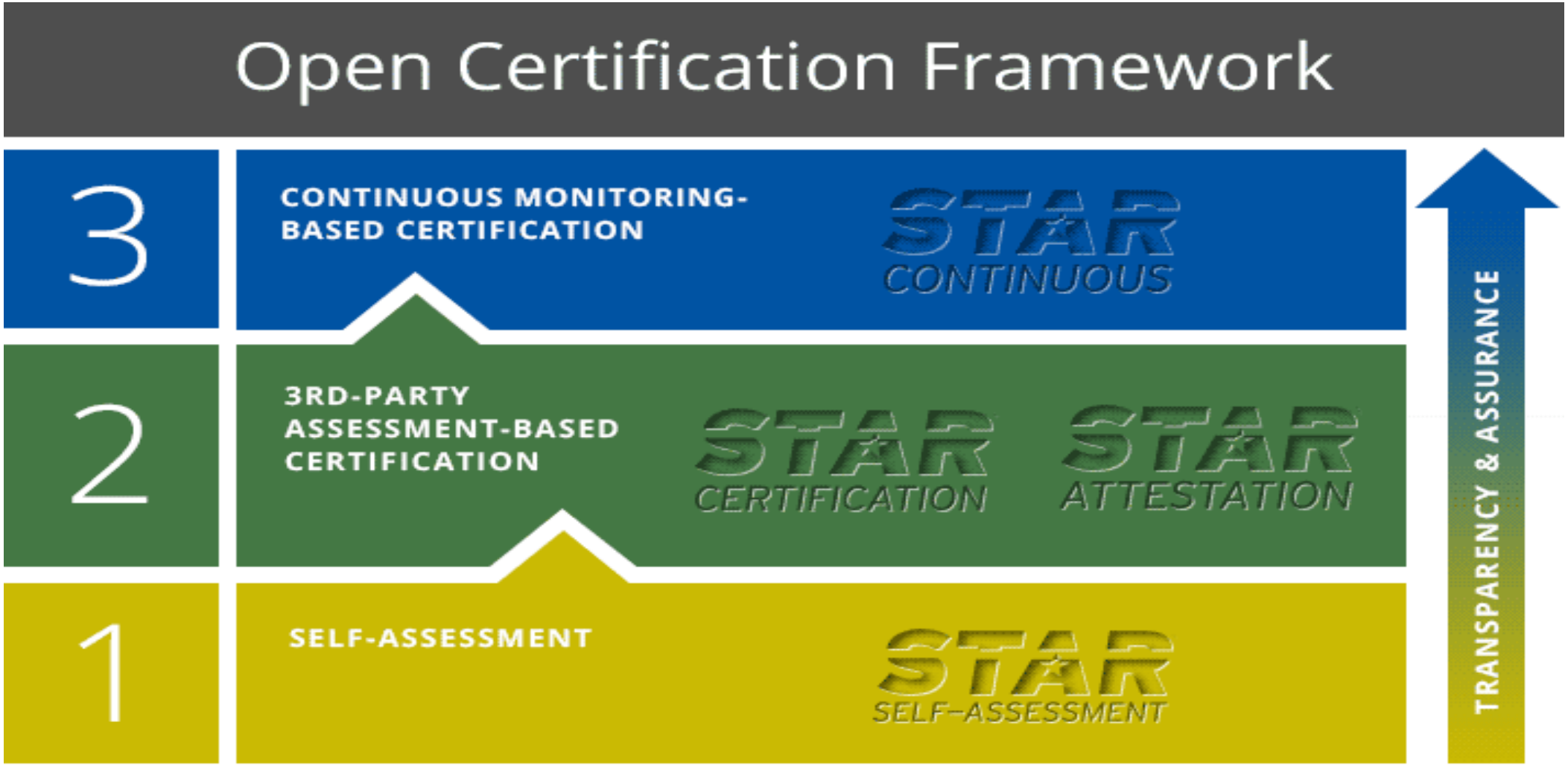
16 domen

133 zabezpieczenia

ZAUFANA TRZECIA STRONA.PL

Open Certification Framework

aruba CLOUD



ZAUFANA TRZECIA STRONA.PL

Podsumowanie

aruba CLOUD