ZAUFANA TRZECIA STRONA.PL

Zarządzanie relacjami z dostawcami

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. Kluczowe czynniki przy wyborze dostawcy usługi z punktu widzenia bezpieczeństwa.
3. Omówienie praktyk i narzędzi do oceny dostawcy i usługi chmurowej dostarczanych przez CSA.
4. Podsumowanie.
5. 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,
- Standardy bezpieczeństwa, jakie powinna spełniać usługa chmurowa i jak możemy sprawdzić, czy te standardy faktycznie spełnia,
- 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 czyli jak uniezależnić się od dostawcy
- Zarządzanie cyklem bezpieczeństwa danych w chmurze

Cloud Native Landscape

2018-11-22T00:26:35Z 8e4f214

See the interactive landscape at l.cncf.io

Greyed logos are not open source

App Definition and Development

Database

Streaming & Messaging

Application Definition & Image Build

Continuous Integration & Delivery

Orchestration & Management

Scheduling & Orchestration

Coordination & Service Discovery

Remote Procedure Call

Service Proxy

API Gateway

Service Mesh

Runtime

Cloud-Native Storage

Container Runtime

Cloud-Native Network

Provisioning

Automation & Configuration

Container Registry

Security & Compliance

Key Management

Cloud

Public

Special

Kubernetes Certified Service Provider

Kubernetes Training Partner

Platform

Certified Kubernetes - Distribution

Certified Kubernetes - Hosted

Certified Kubernetes - Installer

PaaS/Container Service

Observability and Analysis

Monitoring

Logging

Tracing

Chaos Engineering

Serverless

This landscape is intended as a map through the previously uncharted terrain of cloud native technologies. There are many routes to deploying a cloud native application, with CNCF Projects representing a particularly well-traveled path

l.cncf.io

CLOUD NATIVE Landscape

CLOUD NATIVE COMPUTING FOUNDATION

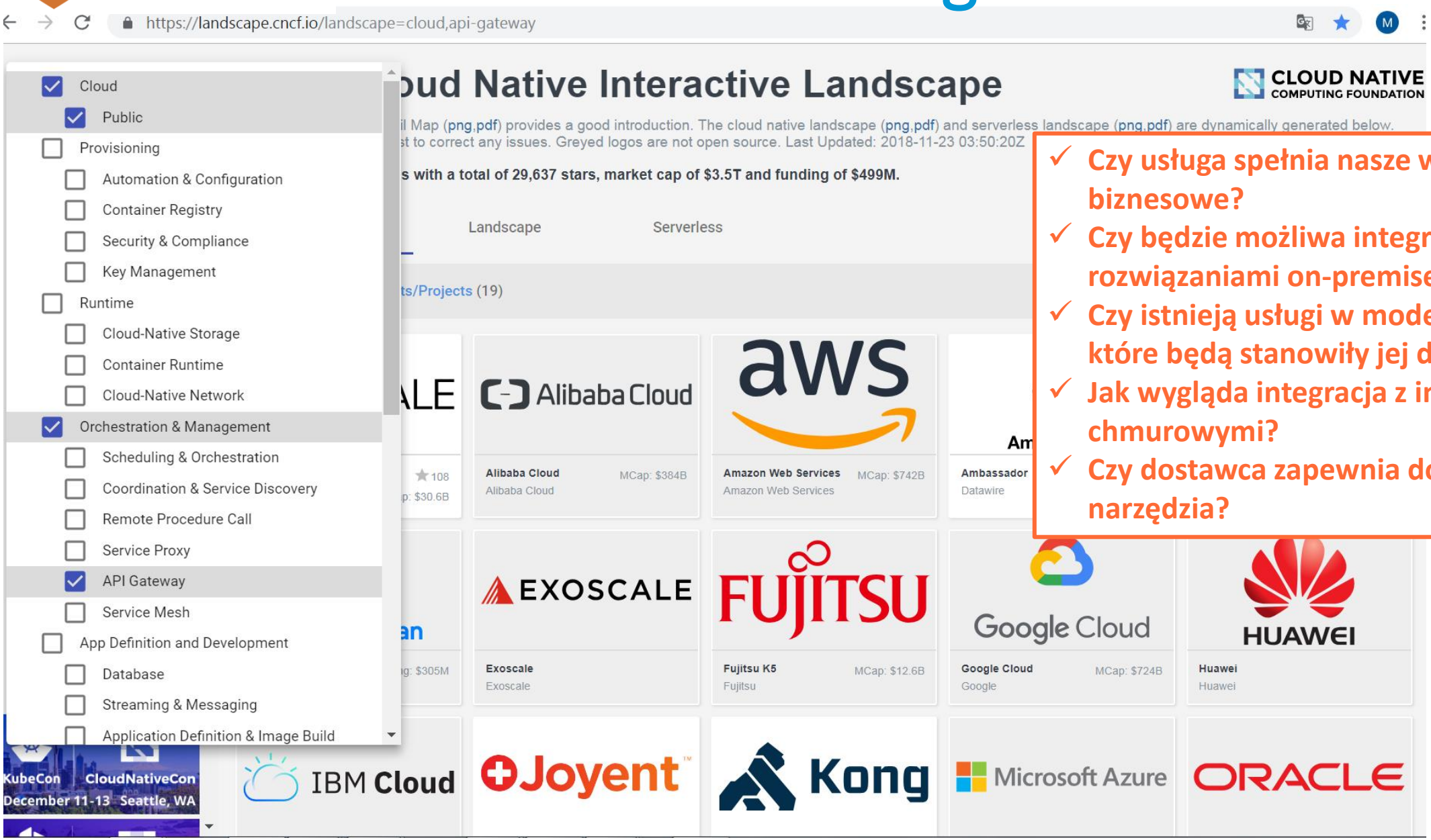
Redpoint

Amplify PARTNERS

ZAUFANA TRZECIA STRONA.PL

Technologia

aruba CLOUD



- ✓ Czy usługa spełnia nasze wymagania biznesowe?
- ✓ Czy będzie możliwa integracja z rozwiązaniami on-premise?
- ✓ Czy istnieją usługi w modelu chmury, które będą stanowiły jej dopełnienie?
- ✓ Jak wygląda integracja z innymi usługami chmurowymi?
- ✓ Czy dostawca zapewnia dodatkowe narzędzia?

ZAUFANA TRZECIA STRONA.PL

Zgodność i certyfikacja

aruba CLOUD

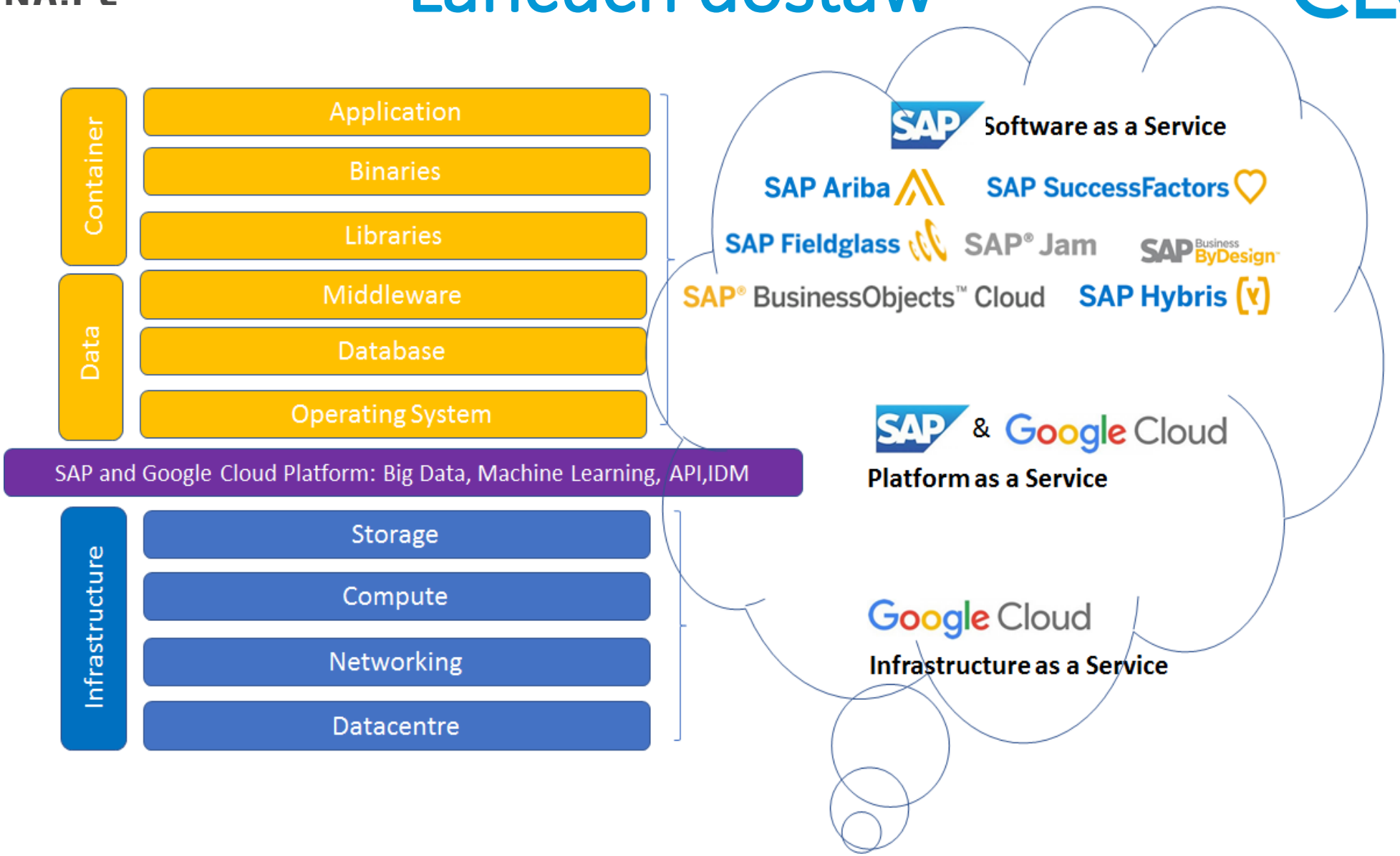
- Lokalizacja danych
- Zabezpieczenia
- Zarządzanie incydentami
- Kodeksy postępowania
- Certyfikaty

www.cloudindustryforum.org

ZAUFANA TRZECIA STRONA.PL

Łańcuch dostaw

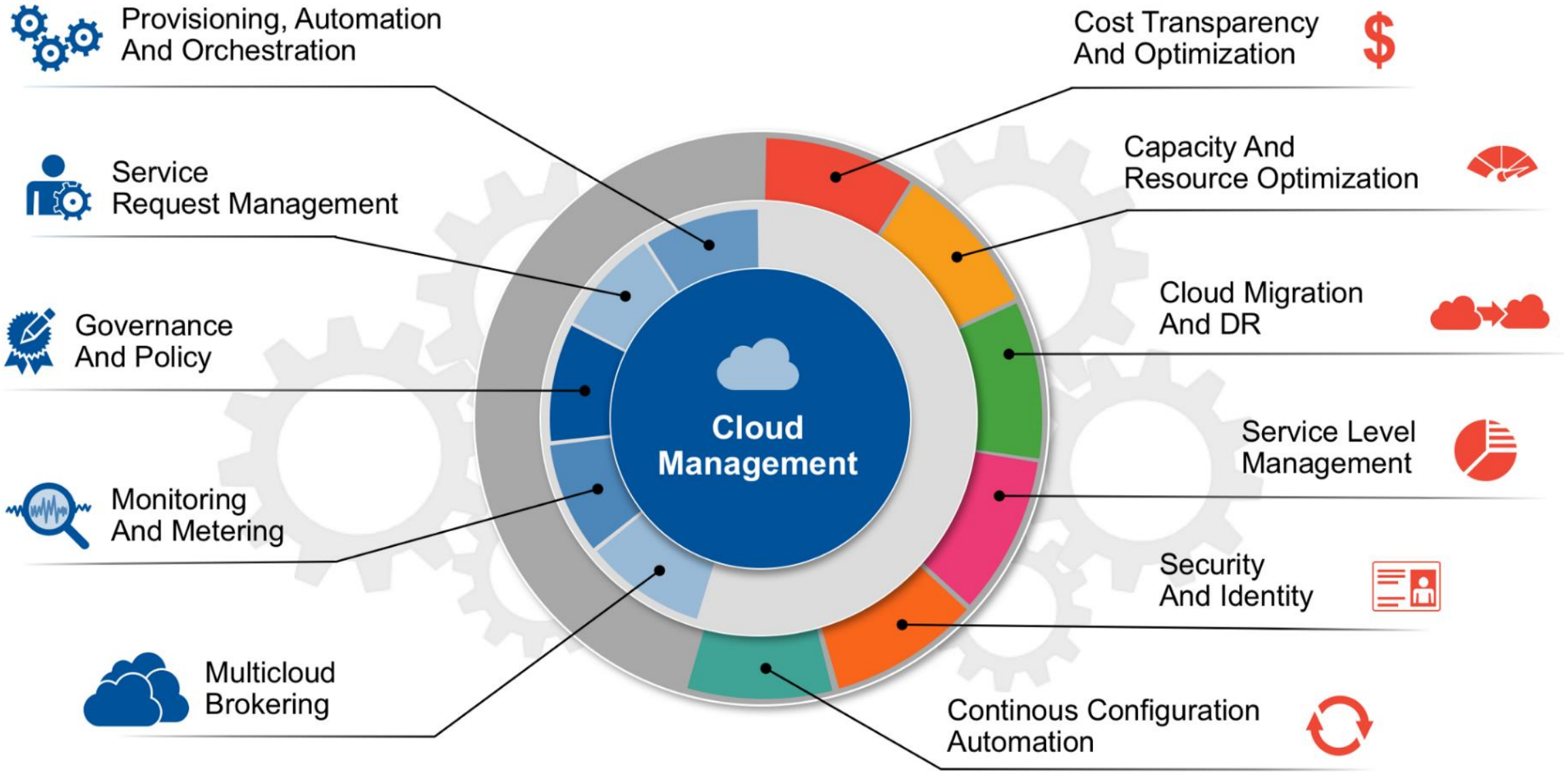
aruba CLOUD



ZAUFANA TRZECIA STRONA.PL

Monitorowanie usług

aruba CLOUD

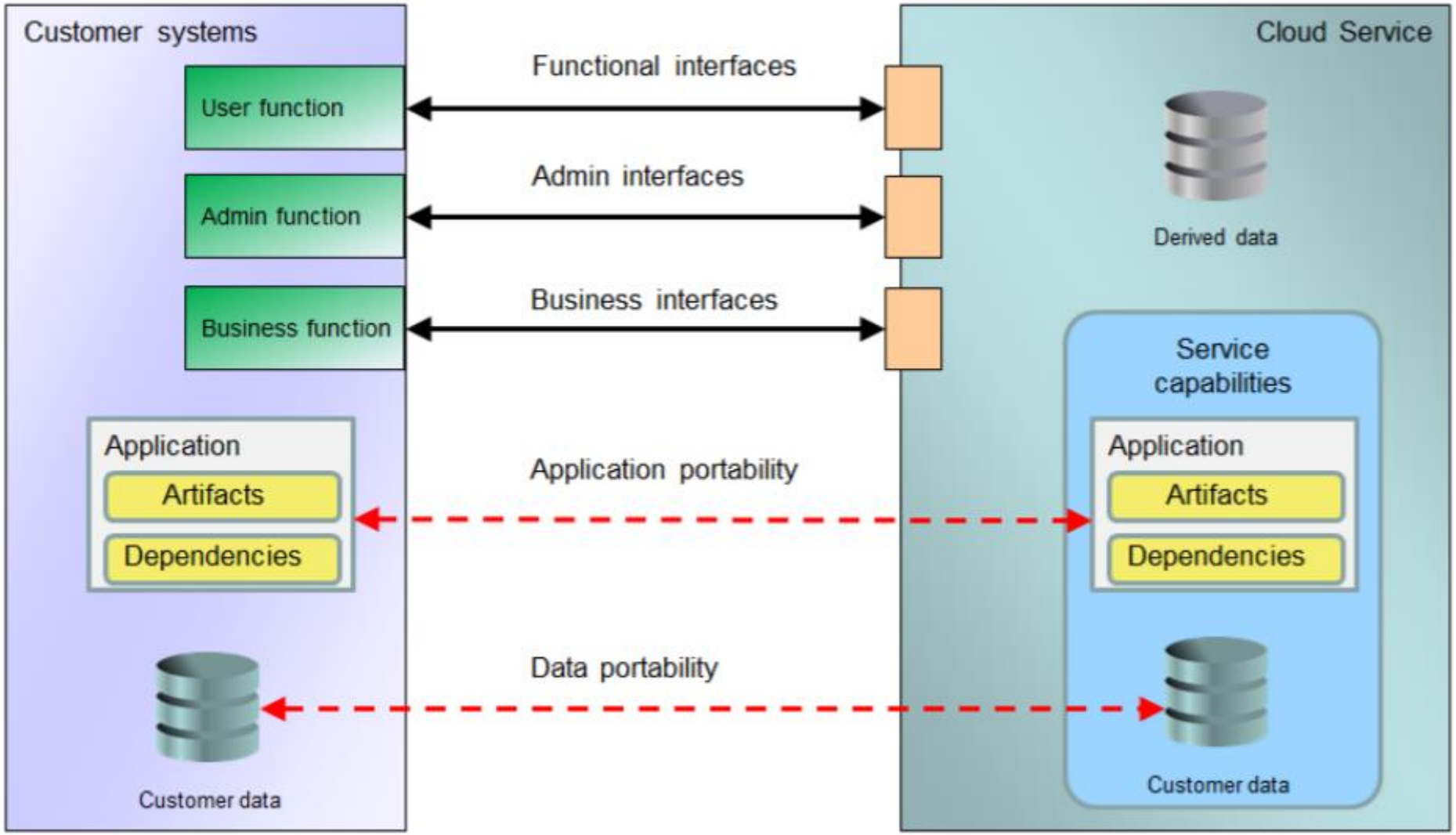


Źródło: Gartner

ZAUFANA TRZECIA STRONA.PL

Uzależnienie od dostawcy

aruba CLOUD

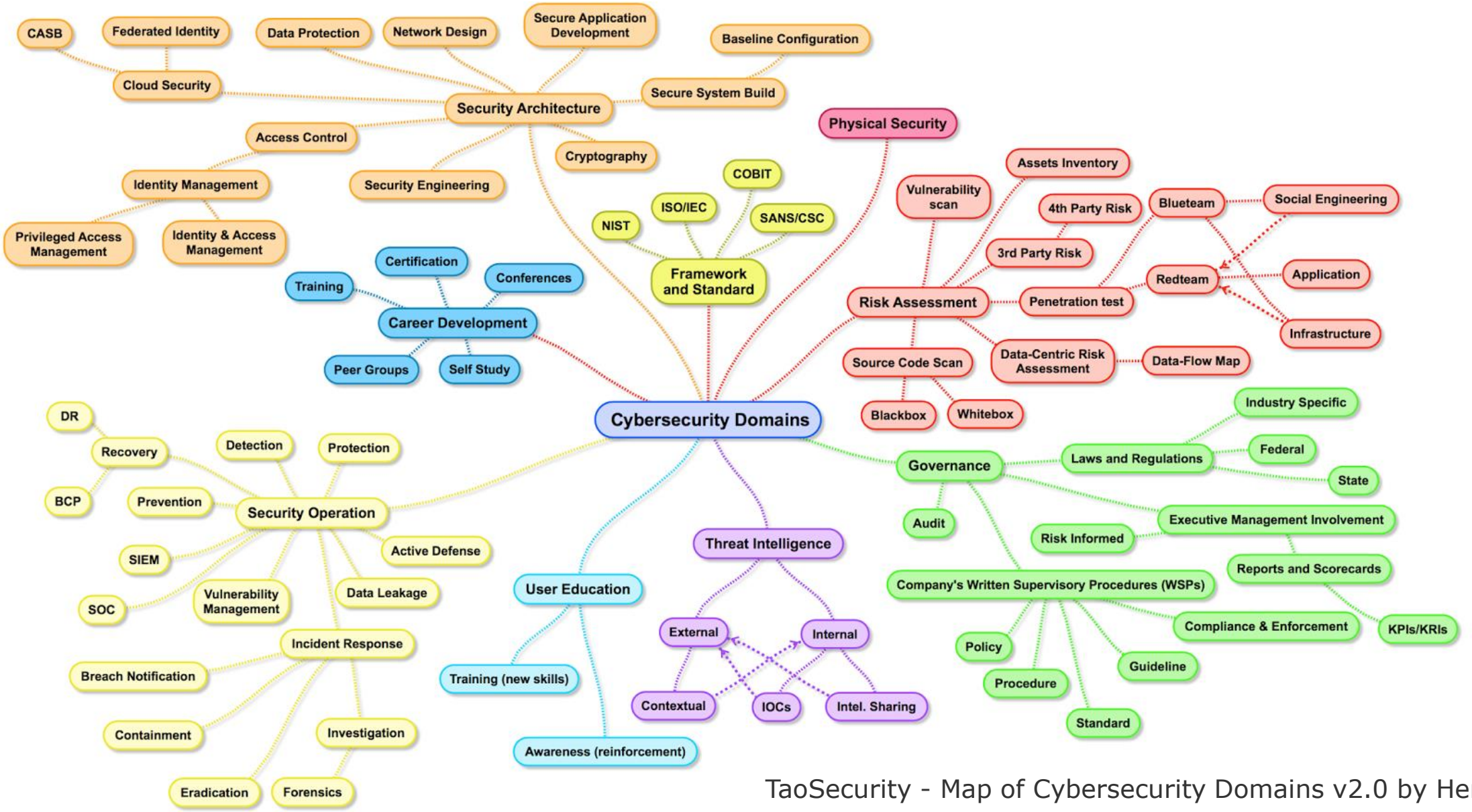


Interoperacyjność i przenaszalność w chmurze – źródło "Interoperability and Portability for Cloud Computing: A Guide"

ZAUFANA TRZECIA STRONA.PL

Cyberbezpieczeństwo

aruba CLOUD

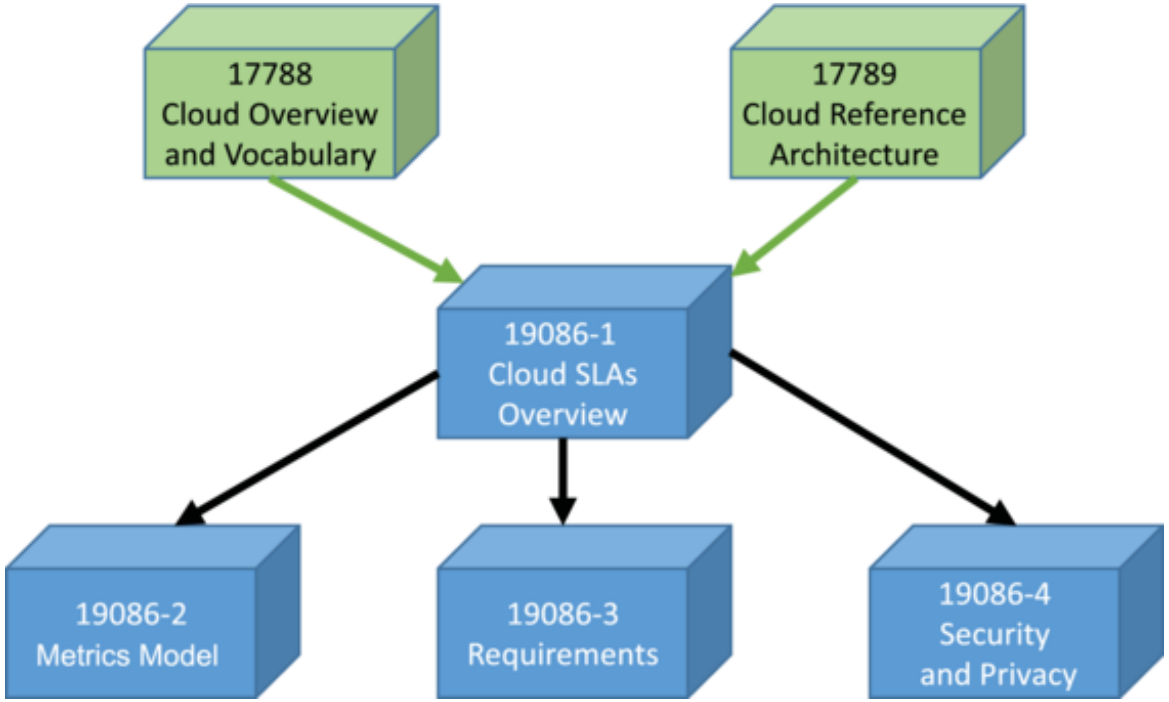


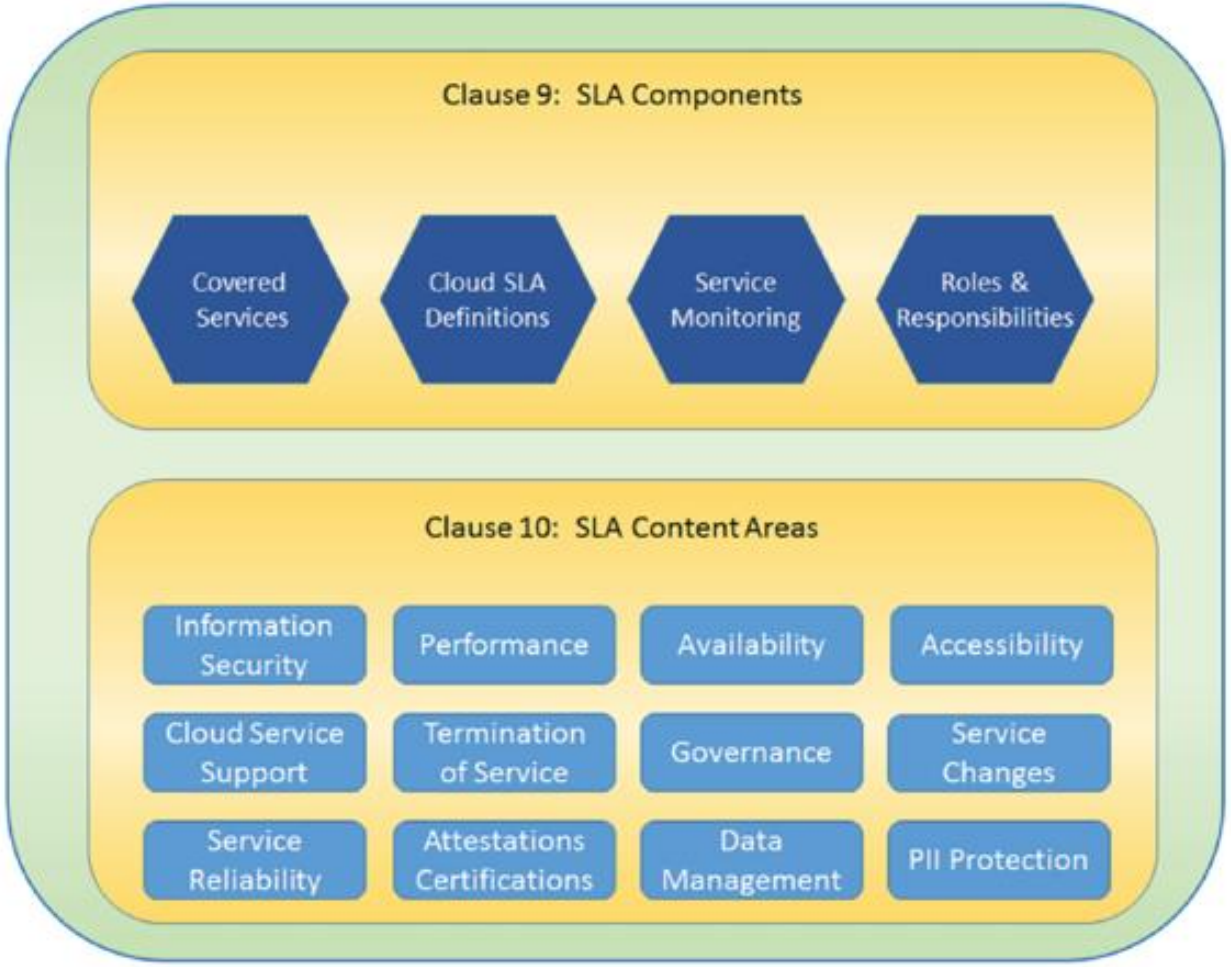
TaoSecurity - Map of Cybersecurity Domains v2.0 by Henry Jiang

ZAUFANA TRZECIA STRONA.PL

Due dilligence

aruba CLOUD

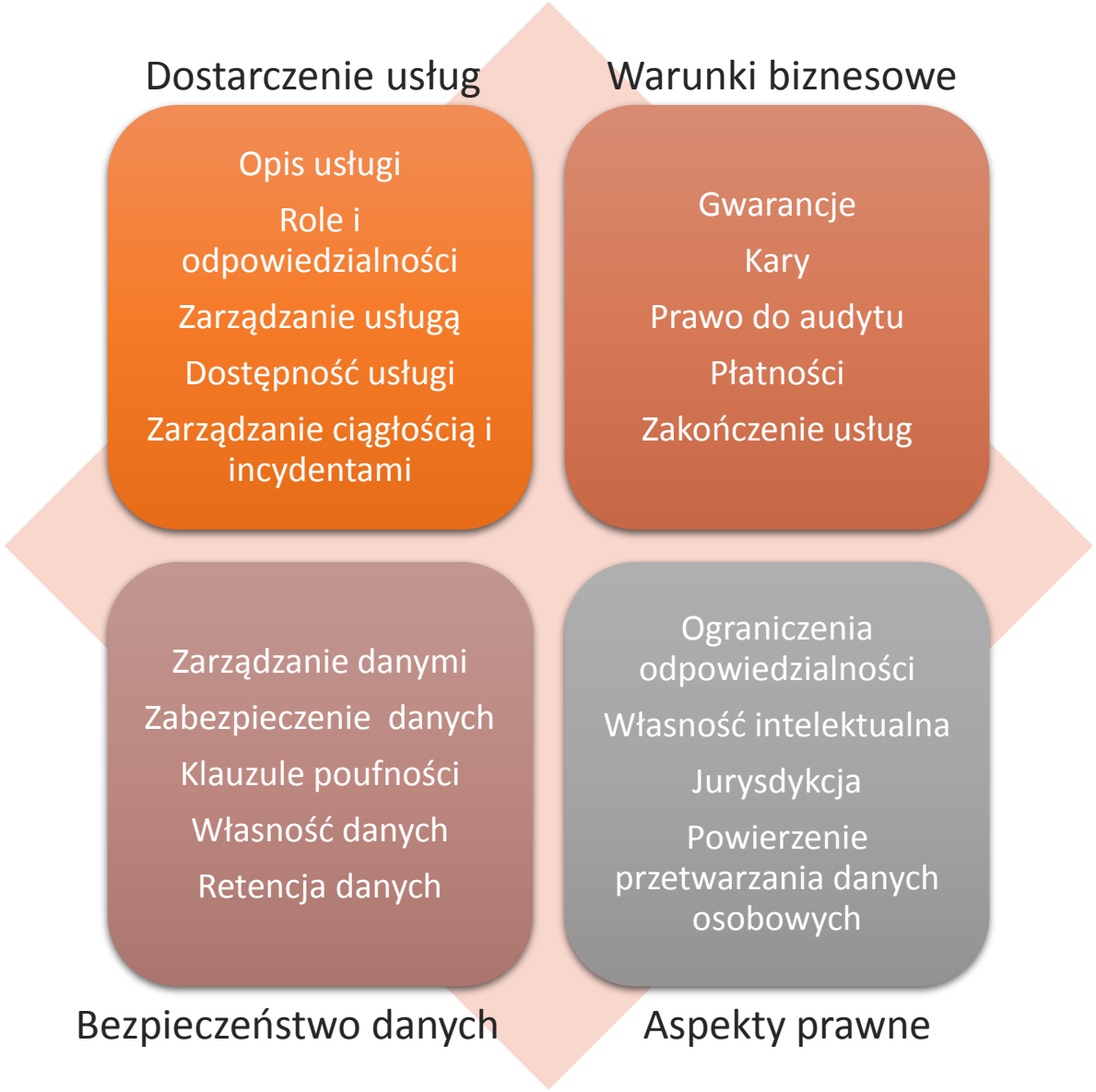




ISO/IEC 19086-1:2016 Information technology — Cloud computing — Service level agreement (SLA) framework

ZAUFANA TRZECIA STRONA.PL

Warunki umowne

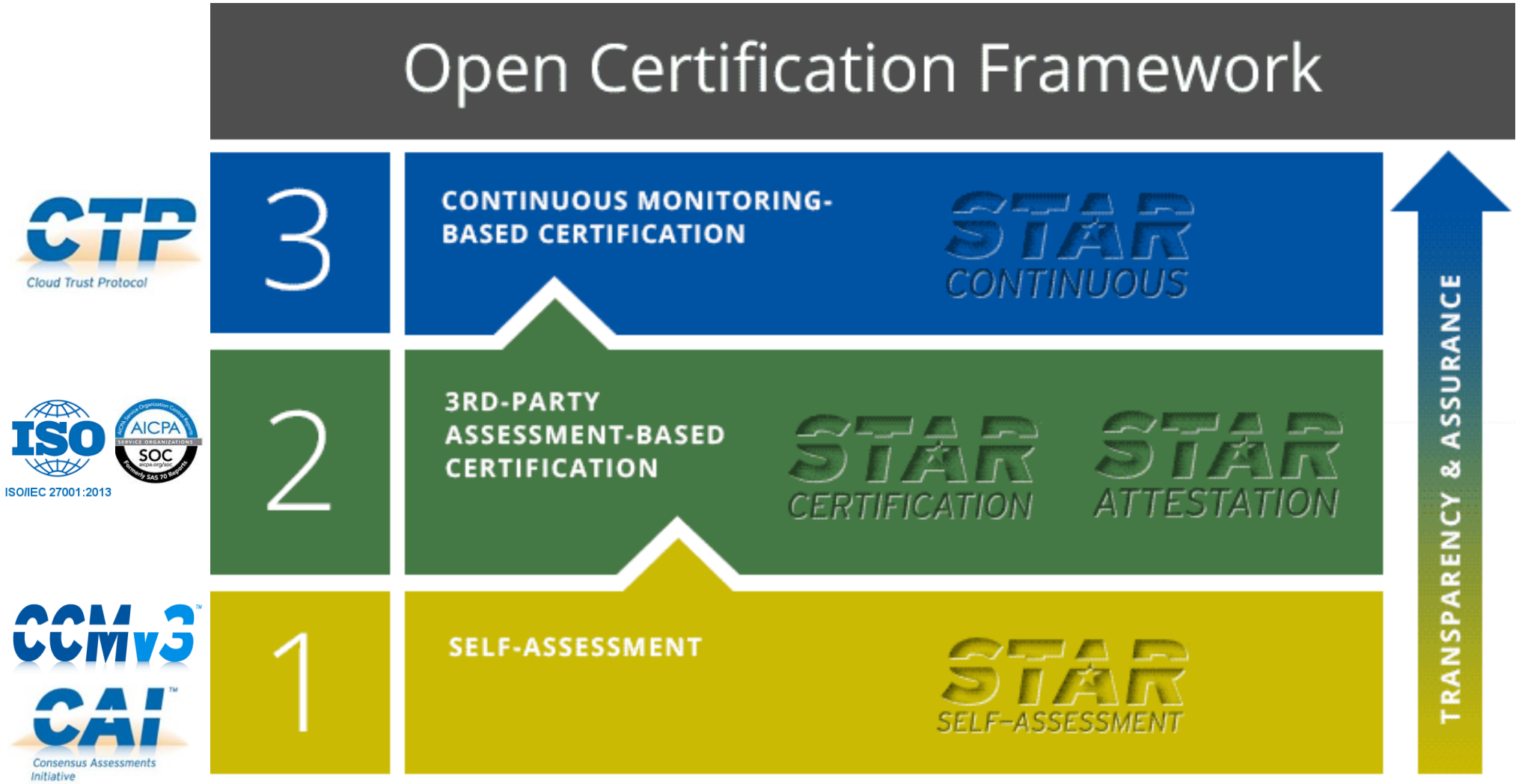


aruba CLOUD

ZAUFANA TRZECIA STRONA.PL

Open Certification Framework

aruba CLOUD



ZAUFANA TRZECIA STRONA.PL

Cloud Control Matrix

aruba CLOUD

16 Domen

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)

ZAUFANA TRZECIA STRONA.PL

Cloud Control Matrix

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

133 zabezpieczenia

ZAUFANA TRZECIA STRONA.PL

Cloud Control Matrix

aruba CLOUD

Datacenter Security (DCS)

- DCS-01: Asset Management
- DCS-02: Controlled Access Points
- DCS-03: Equipment Identification
- DCS-04: Off-Site Authorization
- DCS-05: Off-Site Equipment
- DCS-06: Policy
- DCS-07: Secure Area Authorization
- DCS-08: Unauthorized Persons Entry
- DCS-09: User Access

Encryption & Key Management (EKM)

- EKM-01: Entitlement
- EKM-02: Key Generation
- EKM-03: Sensitive Data Protection
- EKM-04: Storage and Access

Governance and Risk Management (GRM)

- GRM-01: Baseline Requirements
- GRM-02: Data Focus Risk Assessments
- GRM-03: Management Oversight
- GRM-04: Management Program
- GRM-05: Management Support/Involvement
- GRM-06: Policy
- GRM-07: Policy Enforcement
- GRM-08: Policy Impact on Risk Assessments
- GRM-09: Policy Reviews
- GRM-10: Risk Assessments
- GRM-11: Risk Management Framework

133 zabezpieczenia

Source: https://cloudsecurityalliance.org/research/ccm/

ZAUFANA TRZECIA STRONA.PL

Cloud Control Matrix

aruba CLOUD

Human Resources (HRS)

- HRS-01: Asset Returns
- HRS-02: Background Screening
- HRS-03: Employment Agreements
- HRS-04: Employment Termination
- HRS-05: Mobile Device Management
- HRS-06: Non-Disclosure Agreements
- HRS-07: Roles / Responsibilities
- HRS-08: Technology Acceptable Use
- HRS-09: Training / Awareness
- HRS-10: User Responsibility
- HRS-11: Workspace

Identity & Access Management (IAM)

- IAM-01: Audit Tools Access
- IAM-02: Credential Lifecycle / Provision Management
- IAM-03: Diagnostic / Configuration Ports Access
- IAM-04: Policies and Procedures
- IAM-05: Segregation of Duties
- IAM-06: Source Code Access Restriction
- IAM-07: Third Party Access
- IAM-08: Trusted Sources
- IAM-09: User Access Authorization
- IAM-10: User Access Reviews
- IAM-11: User Access Revocation
- IAM-12: User ID Credentials
- IAM-13: Utility Programs Access

133 zabezpieczenia

Source: https://cloudsecurityalliance.org/research/ccm/

ZAUFANA TRZECIA STRONA.PL

Cloud Control Matrix

aruba CLOUD

Infrastructure & Virtualization Security (IVS)

- IVS-01: Audit Logging / Intrusion Detection
- IVS-02: Change Detection
- IVS-03: Clock Synchronization
- IVS-04: Information System Documentation
- IVS-05: Management - Vulnerability Management
- IVS-06: Network Security
- IVS-07: OS Hardening and Base Controls
- IVS-08: Production / Non-Production Environments
- IVS-09: Segmentation
- IVS-10: VM Security - vMotion Data Protection
- IVS-11: VMM Security - Hypervisor Hardening
- IVS-12: Wireless Security
- IVS-13: Network Architecture

Interoperability & Portability (IPY)

- IPY-01: APIs
- IPY-02: Data Request
- IPY-03: Policy & Legal
- IPY-04: Standardized Network Protocols
- IPY-05: Virtualization

Mobility Security (MOS)

- MOS-01: Anti-Malware
- MOS-02: Application Stores
- MOS-03: Approved Applications
- MOS-04: Approved Software for BYOD
- MOS-05: Awareness and Training
- MOS-06: Cloud Based Services
- MOS-07: Compatibility
- MOS-08: Device Eligibility
- MOS-09: Device Inventory
- MOS-10: Device Management
- MOS-11: Encryption
- MOS-12: Jailbreaking and Rooting
- MOS-13: Legal
- MOS-14: Lockout Screen
- MOS-15: Operating Systems
- MOS-16: Passwords
- MOS-17: Policy
- MOS-18: Rem
- MOS-19: Secu
- MOS-20: User

133 zabezpieczenia

Source: https://cloudsecurityalliance.org/research/ccm/

ZAUFANA TRZECIA STRONA.PL

Cloud Control Matrix

aruba CLOUD

Security Incident Management, E-Discovery & Cloud Forensics (SEF)

- SEF-01: Contact / Authority Maintenance
- SEF-02: Incident Management
- SEF-03: Incident Reporting
- SEF-04: Incident Response Legal Preparation
- SEF-05: Incident Response Metrics

Supply Chain Management, Transparency and Accountability (STA)

- STA-01: Data Quality and Integrity
- STA-02: Incident Reporting
- STA-03: Network / Infrastructure Services
- STA-04: Provider Internal Assessments
- STA-05: Supply Chain Agreements
- STA-06: Supply Chain Governance Reviews
- STA-07: Supply Chain Metrics
- STA-08: Third Party Assessment
- STA-09: Third Party Audits

Threat and Vulnerability Management (TVM)

- TVM-01: Anti-Virus / Malicious Software
- TVM-02: Vulnerability / Patch Management
- TVM-03: Mobile Code

133 zabezpieczenia

Source: https://cloudsecurityalliance.org/research/ccm/

ZAUFANA TRZECIA STRONA.PL

Cloud Control Matrix

aruba CLOUD

CCMv3.0.1 CLOUD CONTROLS MATRIX VERSION 3.0.1

Control Domain	CCM V3.0 Control ID	Updated Control Specification	Architectural Relevance						Cloud Service Delivery Model Applicability			Supplier Relationship		Scope Applicability					
			Phys	Network	Compute	Storage	App	Data	SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer	COBIT 5.0	ISO/IEC 27001:2013	ISO/IEC 27002:2013	ISO/IEC 27017:2015	ISO/IEC 270018:2015	PCI DSS v3.2
Application & Interface Security Application Security	AIS-01	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.			X	X	X	X	X	X	X	X		APO09.03 APO13.01 BAI03.01 BAI03.02 BAI03.03 BAI03.05 MEA03.01 MEA03.02	A9.4.2 A9.4.1, 8.1*Partial, A14.2.3, 8.1*partial, A.14.2.7 A12.6.1, A18.2.2	9.4.2 9.4.1 12.6.1 14.2.1 14.2.3 14.2.7 18.2.2	9.4.1 12.6.1 14.2.1		6; 6.5

ZAUFANA TRZECIA STRONA.PL

Consensus Assessment Initiative

aruba CLOUD

CAIQv3.0.1 CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes	CCM v3.0.1 Compliance Mapping		
									COBIT 5.0	ISO/IEC 27001:2013	PCI DSS v3.0
					Yes	No	Not Applicable				
Application & Interface Security *Application Security*	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software					APO09.03 APO13.01 BAI03.01 BAI03.02 BAI03.03 BAI03.05 MEA03.01 MEA03.02	A9.4.2 A9.4.1, 8.1*Partial, A14.2.3, 8.1*partial, A.14.2.7 A12.6.1, A18.2.2	6, 6.5
		AIS-01.2		Do you use an automated source code analysis tool to detect security defects in code prior to production?							
		AIS-01.3		Do you use manual source-code analysis to detect security defects in code prior to production?							
		AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?							
		AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?							

ZAUFANA TRZECIA STRONA.PL

Rejestr STAR

aruba CLOUD

https://cloudsecurityalliance.org/star/registry/?name=

Cloud Security Alliance > STAR > Registry

CSA Security, Trust & Assurance Registry (STAR)

CSA STAR Registry | Validate Authenticity | Submit new Service | Learn More

Search the Registry

Enter search term... Search

is a cloud computing platform for building, deploying and managing applications through a global network of and third-party managed datacenters. It supports both Platform as a Service (PaaS) and Infrastructure as a Service (IaaS) cloud service models, and enables hybr...

SELF-ASSESSMENT | CERTIFICATION | ATTESTATION | C-STAR | CONTINUOUS

Nazwa dostawcy

Submission Info

Registered since: March 30, 2012

ZAUFANA TRZECIA STRONA.PL

Rejestr STAR

aruba CLOUD

Self Assessment

Active as of: April 06, 2016

Consensus Assessments Initiative Questionnaire v3.0.1	Download Supporting Asset #1

Deprecated

Attestation

Active as of: October 01, 2018

STAR Attestation v1	Download

Certification

Active as of: June 20, 2017

STAR Certification v1	Download

ZAUFANA TRZECIA STRONA.PL

Rejestr STAR

Responses to the Cloud Security Alliance Consensus Assessments Initiative Questionnaire

aruba CLOUD

Table of Contents

ZAUFANA TRZECIA STRONA.PL

Rejestr STAR

Responses to CSA CAIQ v3.0.1

aruba CLOUD

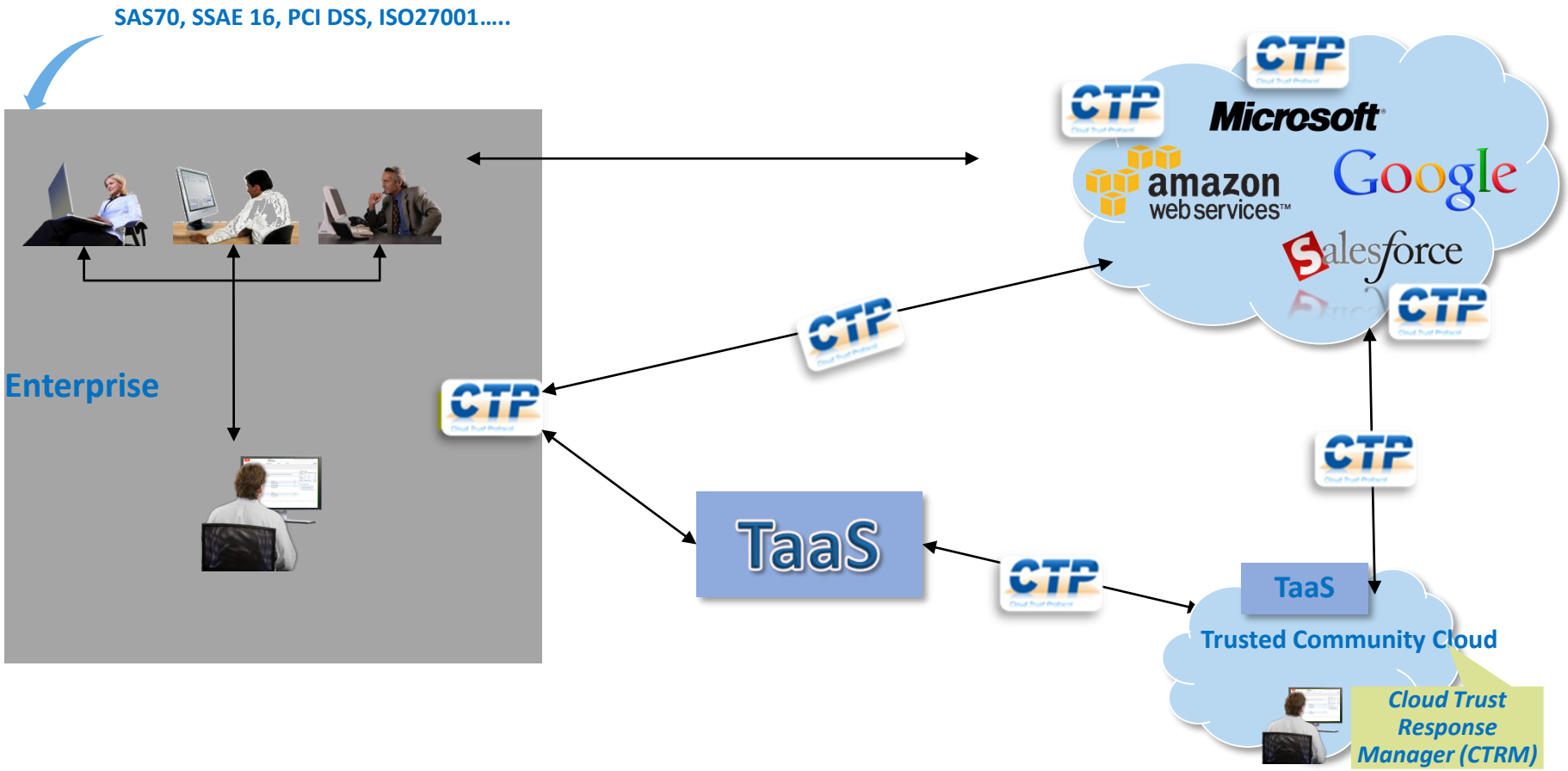
Application and Interface Security: Controls AIS-01 through AIS-04

Control ID in CCM[1]	Consensus Assessment Questions (CCM Version 3.0.1, Final)	Microsoft Azure Response			
		Yes	No	N/A	Notes
AIS-01.1: Application & Interface Security - Application Security	*Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?*	Y			trustworthy foundation concept ensures application security through a process of continuous security improvement with its Security Development Lifecycle (SDL) and Operational Security Assurance (OSA) programs using both Prevent Breach and Assume Breach security postures. Prevent Breach works through the use of ongoing threat modeling, code review and security testing; Assume Breach employs Red-Team / Blue-Team exercises, live site penetration testing and centralized security logging and monitoring to identify and address potential gaps, test security response plans, reduce exposure to attack and reduce access from a compromised system, periodic post-breach assessment and clean state. validates services using third-party penetration testing based upon the OWASP (Open Web Application Security Project) top ten and CREST-certified testers. The outputs of testing are tracked through the risk register, which is audited and reviewed on a regular basis to ensure compliance to security practices.

ZAUFANA TRZECIA STRONA.PL

Cloud Trust Protocol

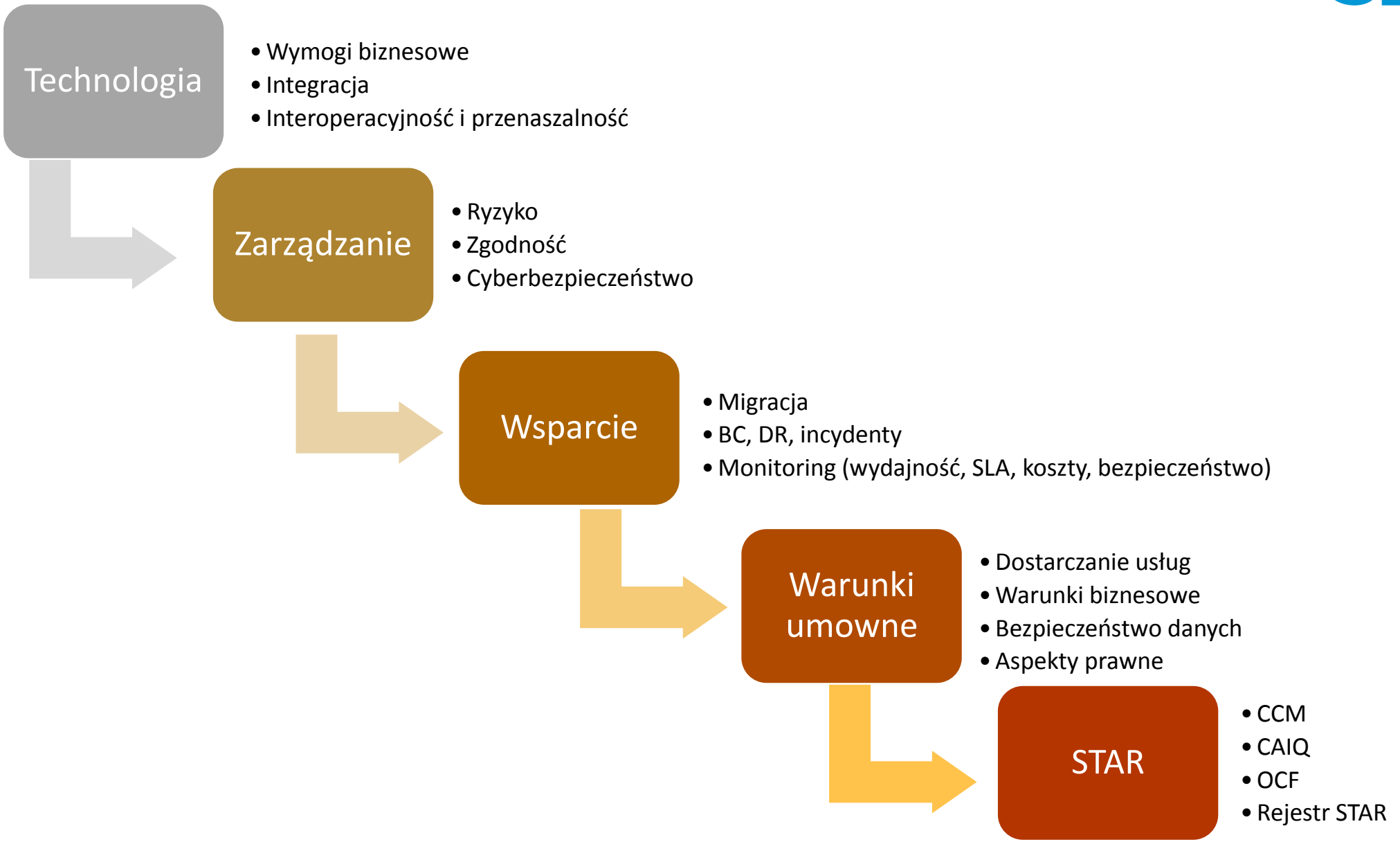
aruba CLOUD



ZAUFANA TRZECIA STRONA.PL

Podsumowanie

aruba CLOUD



ZAUFANA TRZECIA STRONA.PL

aruba CLOUD

Pytania?

Dziękuję za uwagę

Marcin Fronczak