Paweł Rajba
pawel@cs.uni.wroc.pl
http://itcourses.eu/

Information Systems Security

Cloud Computing Security

Agenda

- Introduction, Deployment & Cloud service models
- NIST
  - Definition of cloud computing
  - Cloud Reference Architecture
  - Cloud Evaluation
- Main areas of concern
  - Loss of governance & control
  - Legal & Compliance
  - Cost & capacity control
  - Separation, Lock-in, Data protection
  - Identity & access management
  - Other aspects
- Netskope Cloud Confidence Index

Introduction

> *Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a* ***shared pool*** *of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be* ***rapidly provisioned*** *and released* ***with minimal management effort*** *or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.*

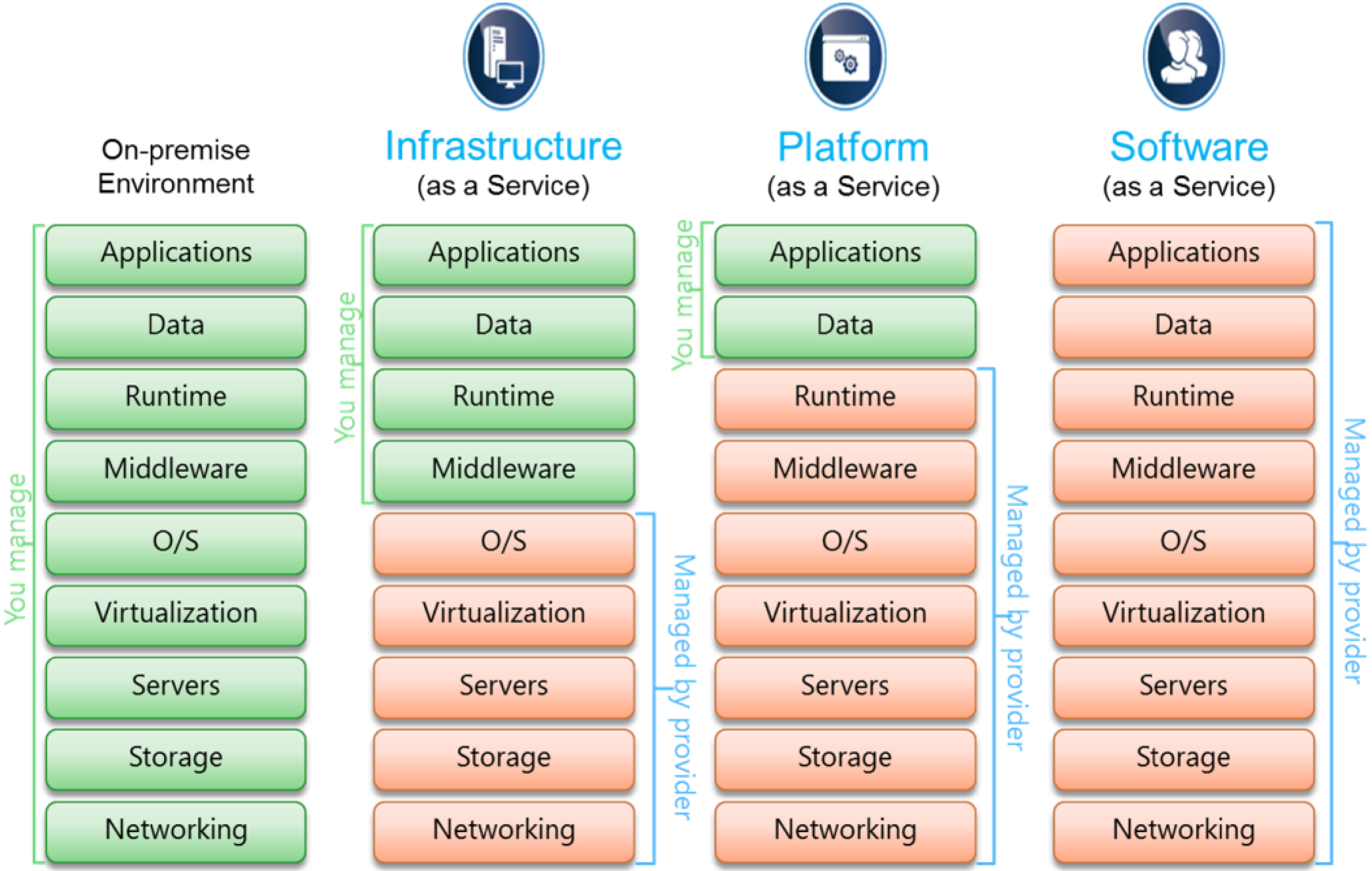
NIST

https://csrc.nist.gov/publications/detail/sp/800-145/final

Deployment models

	Type	Properties
1.	Private cloud	• Outsource or own • Lease or buy • Separate or virtual data center
2.	Community cloud	• Private cloud for a set of users with specific demands • Several stakeholders
3.	Public cloud	• Mega scaleable infrastructure • Available for all
4.	Hybrid cloud	• Combination of two clouds • Usually private for sensitive data and strategic applications

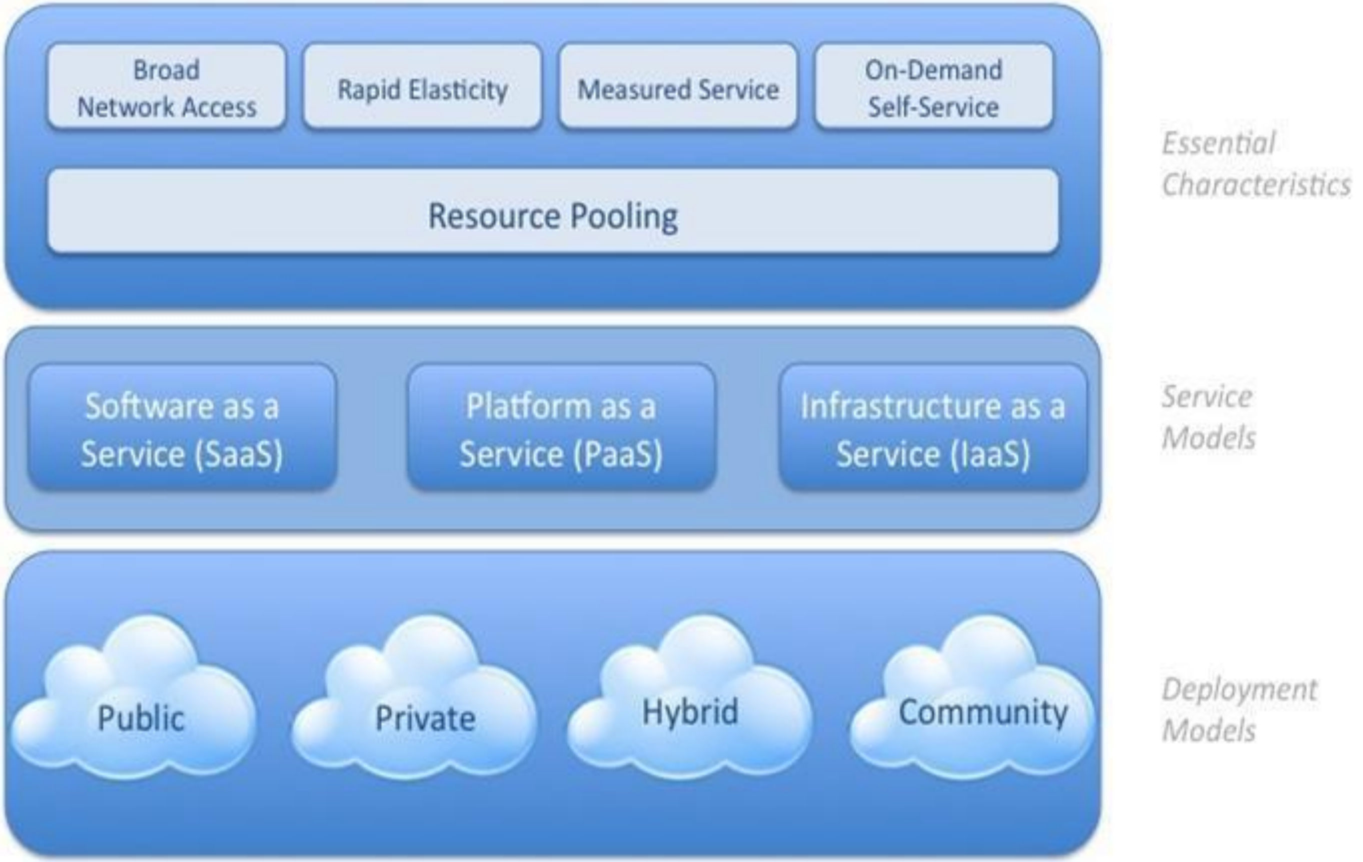
Cloud Service Models



On-premise Environment	Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)
🟩 Applications	🟩 Applications	🟩 Applications	🟥 Applications
🟩 Data	🟩 Data	🟩 Data	🟥 Data
🟩 Runtime	🟩 Runtime	🟥 Runtime	🟥 Runtime
🟩 Middleware	🟩 Middleware	🟥 Middleware	🟥 Middleware
🟩 O/S	🟥 O/S	🟥 O/S	🟥 O/S
🟩 Virtualization	🟥 Virtualization	🟥 Virtualization	🟥 Virtualization
🟩 Servers	🟥 Servers	🟥 Servers	🟥 Servers
🟩 Storage	🟥 Storage	🟥 Storage	🟥 Storage
🟩 Networking	🟥 Networking	🟥 Networking	🟥 Networking

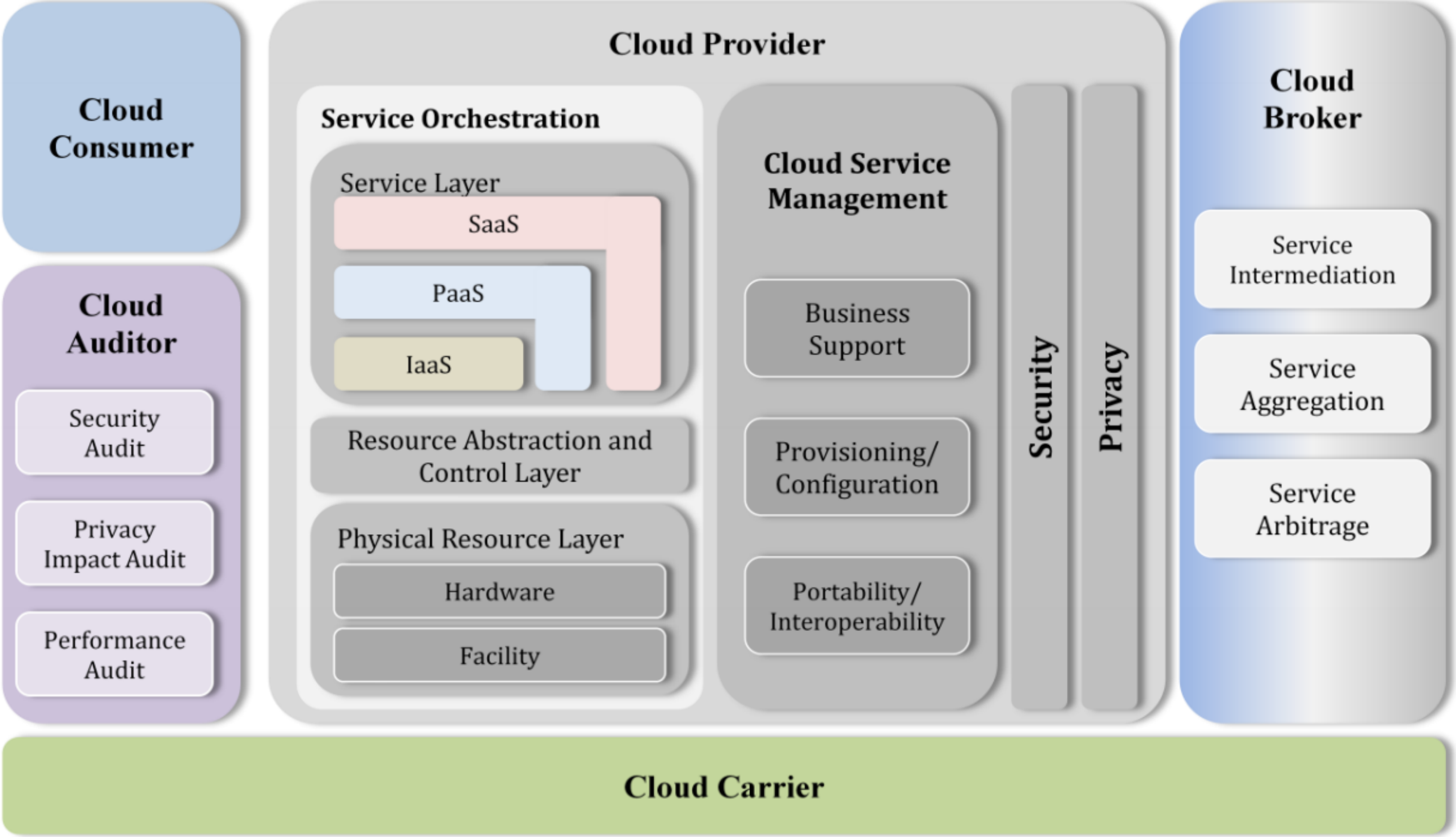
http://blog.binaryinformatics.com/technology/what-is-the-cloud-service-model/

NIST Definition of cloud computing



https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

NIST Cloud Reference Architecture



https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication500-292.pdf

NIST Cloud Evaluation

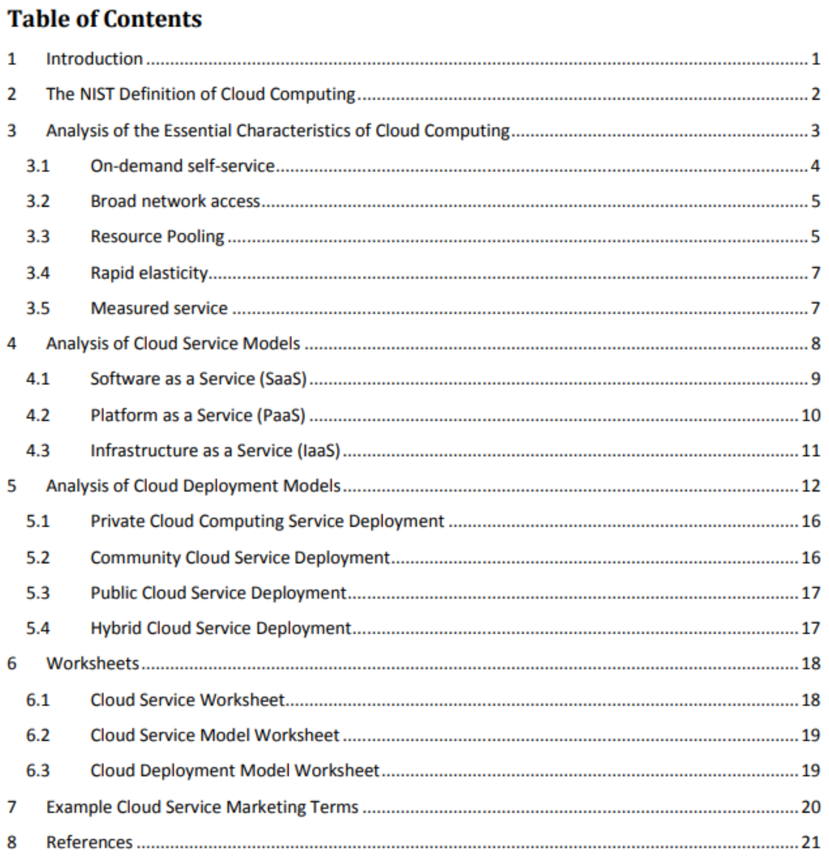


Table of Contents

https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-322.pdf

Main areas of concern

- Loss of governance & control
- Legal & Compliance
- Cost & capacity control
- Separation
- Lock-in
- Identity & access management
- Data protection
- Other aspects

Loss of governance & control

- Risk level is implied by service and deployment models
  - SaaS > PaaS > IaaS
  - Public > Hybrid > Private
- We own data, but it is managed by someone else
- Product development is governed externally
  - Our requirements may not be prioritized
  - Cloud Provider may terminate or fail with some services over time
  - Mainly related to SaaS and PaaS

Legal & Compliance

- When there is a lack of the control, then there is risk of lack the possibility of being compliant
- Infrastructure related regulatory compliance is delegated to the provider
- It is important to understand requirements, especially legal one and make sure the cloud platform is supporting those
  - Privacy related (e.g. famous GDPR, but not only)
  - Location related (e.g. Google is migrating data automatically what might be a problem)
  - Industrial ones (e.g. insurance, healthcare, banking, credit cards)
- Intellectual property challenges who owns the data or parts of the solution
  - E.g. Google Translate

Cost & capacity control

- Very often cost is based on many items, depends on how application is created, so it may be difficult to estimate the TCO
  - Include cost consideration into design
    - https://azure.microsoft.com/en-us/pricing/calculator/
    - https://aws.amazon.com/tco-calculator/
  - Data retension/lifecycle
- Process of ordering services in cloud may be more difficult to control
- Appropriate cost structure and separation is important (e.g. subscription, resource group)

Separation

- The more shared and less controlled environment, the more risks related to separation
- Separation can be considered on different levels:

Application	Infrastructure
• Data separation, e.g. separate servers, databases, schemas (depending on DBMS) • API and UI separation (e.g. in a SaaS, what different roles can see including admin roles)	• Subscription, network security zones, virtual networks, resource groups, virtual machine or container • Platform or runtime separation, e.g. owned vs. shared IIS or Apache

- Consider legal requirements of separation
  - In case of partnership, how much data partners can see of each other

Lock-in

- Very limited support for applications and data portability
  - Can be even prevented by the Cloud Providers
- There are two aspects here:
  - Cloud Provider lock-in
  - Supporting company lock-in (e.g. by competences, contracts or intelectual property)
- It is important to understand the requirements and long term strategy

Lock-in

SaaS	PaaS	IaaS
• High lock-in risks • Unknown internal structure • Lack of tools to make migration so, *additional efforts needed to write tailored solutions* • Risk of additional cost of migration (e.g. extensive data load) • A new solution implies changed UX, trainings, many others	• High-medium risks • Solution build on platform use unique platform components and services, usually not easily portable • Even standard runtime (e.g. Java) may be different for security or other reasons	• Medium-low risks, however: • VM images might be incompatible • Cheaper data services may be used (key-value pairs) which are not portable • Underlying network & security zones architecture might be not portable • Additional security services might be use (key vaults, access control) which are not portable

IAM

- Identities storage and lifecycle
  - Federation strategy
  - If stored in cloud, check compliance with requirements
- Permissions storage, lifecycle and management
  - Storage for permissions, sometimes tricky for SaaS
- Isolation level of identities and permissions
  - Including administration perspective
- Provided authentication methods
  - Protocols supporting federation and details of those (e.g. OIDC), support for offline mode
  - Multifactor authentication

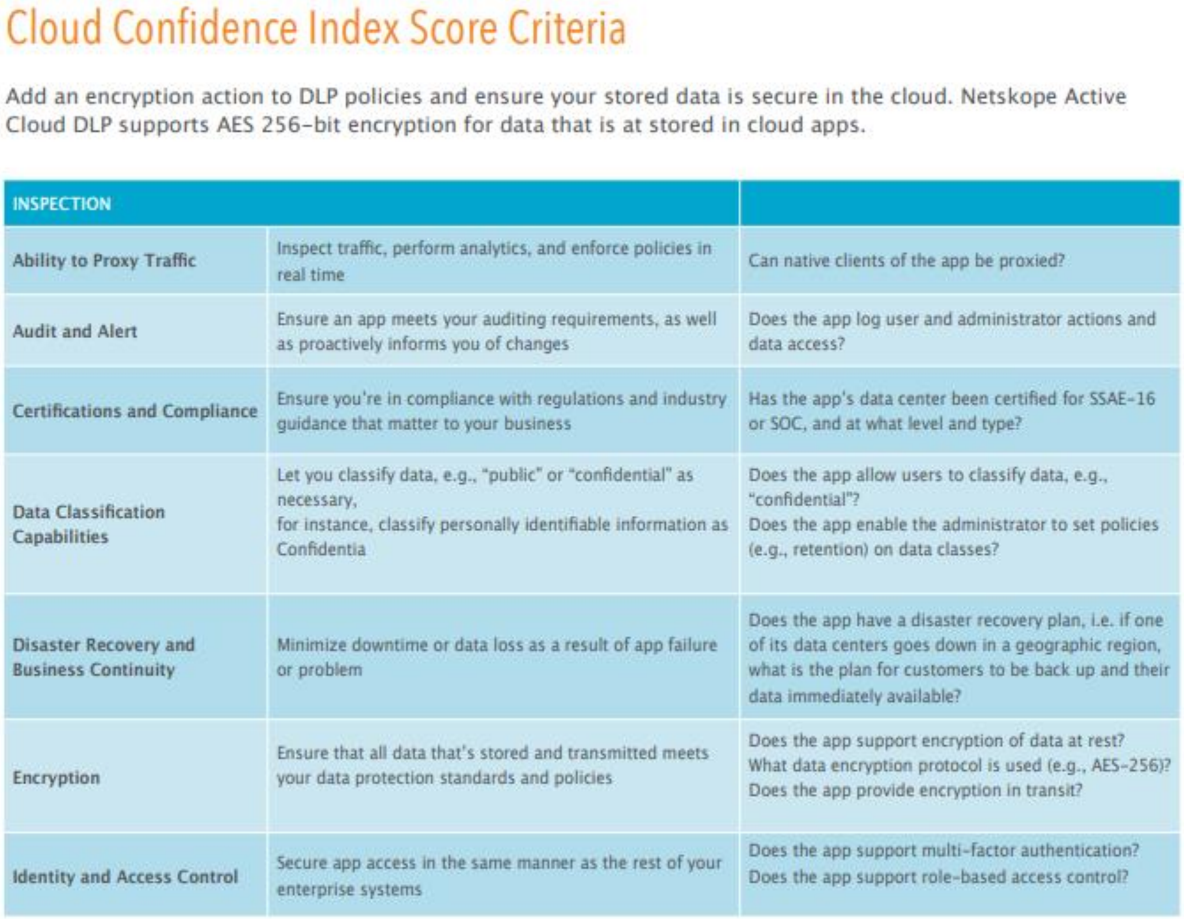
Data protection

- Having data outside premises, we need to trust it is protected on the expected level
- How to increase the trust and where are the risks?
  - Protection in storage
  - Protection in transit
  - Key protection
  - Expect reports from third-party companies of audit or pentests
- Vulnerability scans
  - Conducting such scans are more complicated in public clouds

Other aspects

- Backup & recovery, continuity, uptime & SLAs
- Auditing & Monitoring
  - Do we have access into audit results?
  - Connection to SIEM solutions (internal/external), Visual dashboards
  - Access to different logs & audits & backups
    - For instance, in the finance we want to know who access financial confidential data
  - Application layer vulnerability scans: permitted/conducted/reported
  - Network penetration tests (for supplier delivered infrastructure)
  - Access to action audit logs for enterprise data and user information
- Forensic & Non-repudiation
  - Breach disclosure policy
  - Investigation support in case of breach or compromise of data or users
  - Third-party investigation support in case of breach or compromise of data or users

Netskope Cloud Confidence Index



Cloud Confidence Index Score Criteria

Add an encryption action to DLP policies and ensure your stored data is secure in the cloud. Netskope Active Cloud DLP supports AES 256-bit encryption for data that is at stored in cloud apps.

INSPECTION		
Ability to Proxy Traffic	Inspect traffic, perform analytics, and enforce policies in real time	Can native clients of the app be proxied?
Audit and Alert	Ensure an app meets your auditing requirements, as well as proactively informs you of changes	Does the app log user and administrator actions and data access?
Certifications and Compliance	Ensure you're in compliance with regulations and industry guidance that matter to your business	Has the app's data center been certified for SSAE-16 or SOC, and at what level and type?
Data Classification Capabilities	Let you classify data, e.g., "public" or "confidential" as necessary, for instance, classify personally identifiable information as Confidentia	Does the app allow users to classify data, e.g., "confidential"? Does the app enable the administrator to set policies (e.g., retention) on data classes?
Disaster Recovery and Business Continuity	Minimize downtime or data loss as a result of app failure or problem	Does the app have a disaster recovery plan, i.e. if one of its data centers goes down in a geographic region, what is the plan for customers to be back up and their data immediately available?
Encryption	Ensure that all data that's stored and transmitted meets your data protection standards and policies	Does the app support encryption of data at rest? What data encryption protocol is used (e.g., AES-256)? Does the app provide encryption in transit?
Identity and Access Control	Secure app access in the same manner as the rest of your enterprise systems	Does the app support multi-factor authentication? Does the app support role-based access control?

https://www.netskope.com/resources/netskope-cci-audit
http://go.netskope.com/rs/netskope/images/NS-Cloud-Confidence-Index-DS-00.pdf

DEMO

- Review Azure AppService security capabilities
  - Access Control
  - Authentication/Authorization
  - Application Insights
  - Identity
    - Allow to authenticate an App Service in other services (e.g. KeyVault)
  - Backup
  - SSL settings
  - Alerts
  - Log Stream

References & further reading

- Cloud Computing Risk Assessment
  - https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment
- Cloud Computing Reference Architecture
  - https://www.nist.gov/publications/nist-cloud-computing-reference-architecture
- Evaluation of Cloud Computing Services Based on NIST 800-145
  - https://www.nist.gov/sites/default/files/documents/2017/05/31/evaluation_of_cloud_computing_services_based_on_nist_800-145_20170427clean.pdf
- The Treacherous 12
  - https://downloads.cloudsecurityalliance.org/assets/research/top-threats/Treacherous-12_Cloud-Computing_Top-Threats.pdf