Separation in the Cloud

Architecture

Virtualisation

Separation in the cloud

- Software can be used to divide the resources of a single physical element into multiple elements.

- Virtualisation affords the resources of a physical host to create numerous virtual elements of virtual machines (VMs).

- VMs execute their own operating system and behave as if they an independent single system when they actually a fraction of the resources of a single host.

Hypervisor

Separation in the cloud

- A hypervisor is software or software layer that affords a physical systems to be subdivided into numerous virtual elements.
- The virtual machine monitor (VMM) manages the various virtual elements or virtual machines and maintains logical separation between them.
- For example, if one virtual machine was to crash, it would not bring down other virtual machines being managed by the virtual machine monitor or hypervisor.

Multi-tenancy

Separation in the cloud

- Cloud providers have extensive computing resources that they subdivide and offer to clients on-demand.
- Costs are shared between clients, rather than being the burden of a single company or just a few companies.
- Cloud providers could purchase independent, dedicated, physical compute infrastructure and get companies to pay for it - physically separating the resources from one company to another.
- Cloud providers instead purchase physical compute infrastructure and subdivide it between companies, virtually, consequently the separation is not physical but logical.

Concerns of Logical Seperation

Concerns of logical separation

Architecture

Physical Security

Data Leakage

Malicious Tenants

Mixed Data

Attack Surface

Access Controls

Monitoring Controls

Physical security

Concerns of logical separation

- Cloud providers can invest in physical security far more than most companies.
- Continuous monitoring is used to determine if there is any obvious failure in compliance or risk.
- Security over the supply-chain of physical components that can be interfered with by different attackers, larger companies can address better than most companies.

Data Leakage

Concerns of logical separation

- Encryption can be used to protect data at rest as to mitigate the risk of others consuming date.
- Encryption can be used to protect data in transit as it passes between elements in the system.
- Cloud providers can also provide proprietary solutions to further strengthen protections for data at rest and in transit.

Malicious Tenants

Concerns of logical separation

- Malicious tenants could consume resources to detriment of other tenants.

- Non-malicious, ignorant tenants could compromise infrastructure through poor configuration.

- Need to understand tactics and policy employed by cloud provider, such as least privilege.

Mixed Data

Concerns of logical separation

- Data could be mixed at the application level or within databases and other stores, including back-ups.
- Service Level Agreements (SLAs) can be used to enforce contractual requirements.
- Independent certification and/or audits can be used to minimise undesirable mixing of data.

Attack Surface

Concerns of logical separation

- Virtualised environments have larger attack surface as several virtual elements could be comprised on a single host.
- Determine tactics used by cloud provider to limit attack surface, including separation of activities.

Access Controls

Concerns of logical separation

- Access controls are crucial in ensuring security of data.
- Service Level Agreements (SLAs) and independent audits can be used to ensure access controls are being properly generated and maintained.

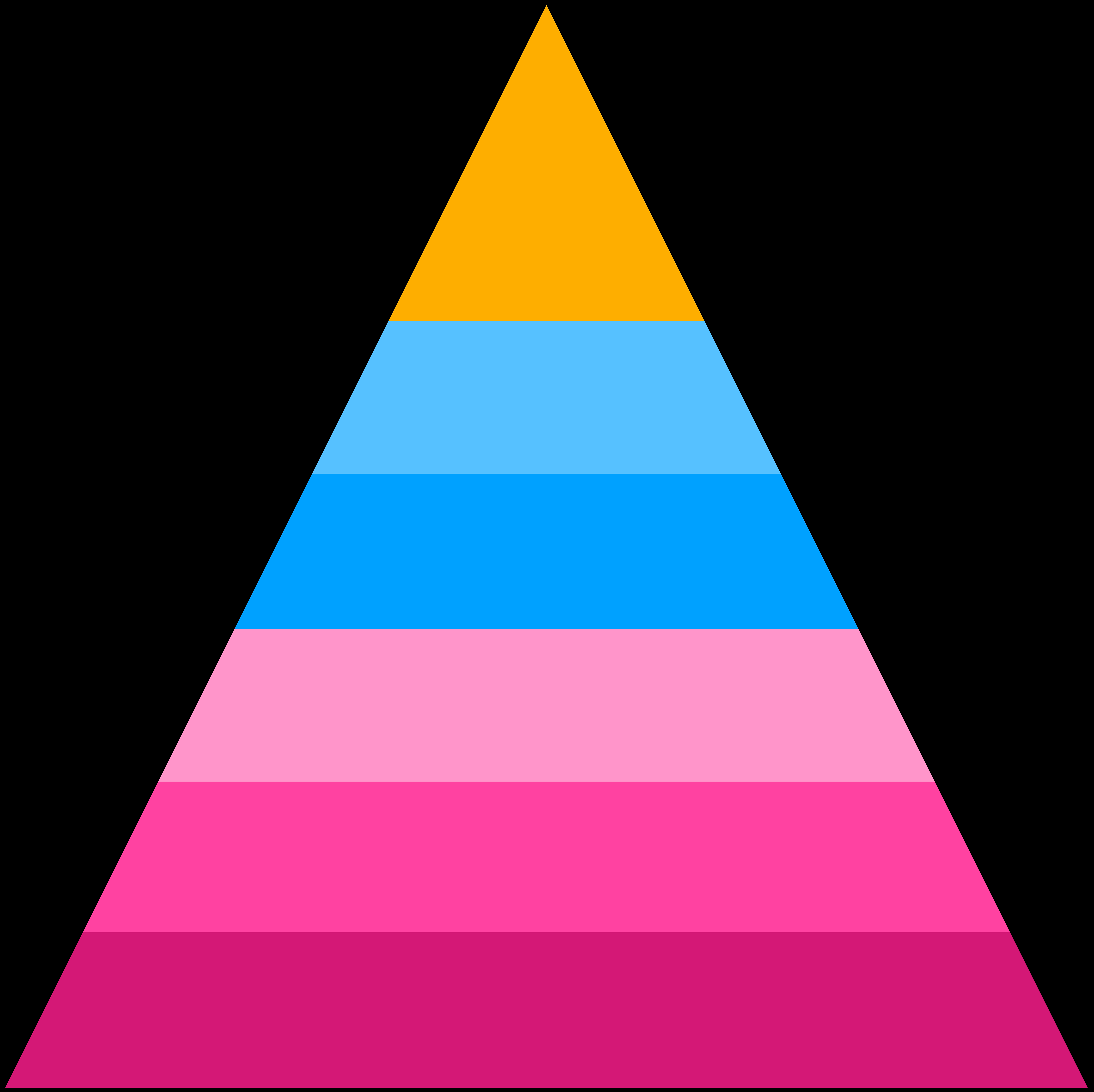
Monitoring Controls

Concerns of logical separation

- Concerns that cloud providers may not log important actions and elements that are relevant to a given company.
- Ensure cloud provider supports enterprises to monitor and log aspects important to enterprise.

Responsibility in the Cloud

Cloud Provider



Applications

Network controls

Operating system

Hosting infrastructure

Network infrastructure

Datacentre

	SaaS	PaaS	IaaS	Private
Governance of Data	○	○	○	○
Endpoints	○	○	○	○
Access Management	○	○	○	○
Identity Management	○	○	○	○
Applications	○	○	○	○
Network controls	○	○	○	○
Operating system	○	○	○	○
Hosting infrastructure	○	○	○	○
Network infrastructure	○	○	○	○
Datacentre	○	○	○	○

Determine the cloud provider and enterprise responsibilities for given elements in the infrastructure.

	SaaS	PaaS	IaaS	Private
Governance of Data	○	○	○	○
Endpoints	○	○	○	○
Access Management	○	○	○	○
Identity Management	○	○	○	○
Applications	○	○	○	○
Network controls	○	○	○	○
Operating system	○	○	○	○
Hosting infrastructure	○	○	○	○
Network infrastructure	○	○	○	○
Datacentre	○	○	○	○

	SaaS	PaaS	IaaS	Private
Governance of Data	●	●	●	●
Endpoints	●	●	●	●
Access Management	●	●	●	●
Identity Management	○	○	●	●
Applications	○	○	●	●
Network controls	○	○	●	●
Operating system	○	○	●	●
Hosting infrastructure	○	○	○	●
Network infrastructure	○	○	○	●
Datacentre	○	○	○	●

	SaaS	PaaS	IaaS	Private
Governance of Data	🔵	🔵	🔵	🔵
Endpoints	🔵	🔵	🔵	🔵
Access Management	🔵	🔵	🔵	🔵
Identity Management	○	○	🔵	🔵
Applications	🟠	○	🔵	🔵
Network controls	🟠	○	🔵	🔵
Operating system	🟠	🟠	🔵	🔵
Hosting infrastructure	🟠	🟠	🟠	🔵
Network infrastructure	🟠	🟠	🟠	🔵
Datacentre	🟠	🟠	🟠	🔵

	SaaS	PaaS	IaaS	Private
Governance of Data	🔵	🔵	🔵	🔵
Endpoints	🔵	🔵	🔵	🔵
Access Management	🔵	🔵	🔵	🔵
Identity Management	🟣	🟣	🔵	🔵
Applications	🟠	🟣	🔵	🔵
Network controls	🟠	🟣	🔵	🔵
Operating system	🟠	🟠	🔵	🔵
Hosting infrastructure	🟠	🟠	🟠	🔵
Network infrastructure	🟠	🟠	🟠	🔵
Datacentre	🟠	🟠	🟠	🔵

Separation in the Cloud

Architecture