

Security and Privacy of Cloud Computing

Architecture

Security and Privacy

- Enterprises must carefully consider and plan the transition to cloud computing infrastructure.
- Enterprises must actually comprehend and appreciate the cloud computing infrastructure.
- Enterprises need to understand their own security and privacy requirements as to ensure cloud providers can satisfy them.
- Enterprises must not overlook their own security and privacy requirements on premises when relying on cloud providers.
- Enterprises must remain accountable for the security and privacy of data and applications implemented and deployed in cloud computing infrastructure.

The Good,
the Bad
and the Ugly.

servicenow®

The Good,
the Bad
and the Ugly.

The Good

Cloud computing



Specialist
Staff

Uniform
Platform

Concentration

Availability
and Access

Recovery

The Good

Cloud computing



Specialist
Staff

- Cloud providers can **attract and retain specialised and expert staff** in security, privacy, infrastructure, compliance ... than traditional companies.
- **Expertise that remains focused** on their specialism as they are not burden with other duties.
- **Affords infrastructure refinement** as expert staff can see multiple clients, consider emerging problems and address them.

The Good

Cloud computing



Specialist
Staff

Uniform
Platform

Concentration

Availability
and Access

Recovery

The Good

Cloud computing



Uniform Platform

- Uniform platform allows cloud providers to **harden and tighten existing elements**.
- **Automation of security management** controls, such as auditing and vulnerability testing.
- **Improved infrastructure management** improves availability and reliability, for example load balancing.
- **Operational compliance for specific domains**, such as health and finance.

The Good

Cloud computing



Specialist
Staff

Uniform
Platform

Concentration

Availability
and Access

Recovery

The Good

Cloud computing



Concentration

- **Data concentrated in central infrastructure** instead of scattered across distributed elements.
- **Applications and services can be tailored to access concentrated data** improving confidentiality of data.
- **Increased endpoints** affording improved availability and productivity.

The Good

Cloud computing



Specialist
Staff

Uniform
Platform

Concentration

Availability
and Access

Recovery

The Good

Cloud computing



Availability and Access

- Disaster recovery and redundancy support recovery with **on-demand access to resource**.
- **Increased availability improves integrity of data** as individuals can refine data, for example update records.
- **Capture data more rapidly** when incidents occur to address problems.

The Good

Cloud computing



Specialist
Staff

Uniform
Platform

Concentration

Availability
and Access

Recovery

The Good

Cloud computing



Recovery

- **Geographical compliance** can be supported with multiple sites provided by cloud provider.
- Repository and **diverse back-up policies, strategy and location** to back-up data.
- **Restoration often more rapid** when coupled with uniform platform, specialised staff and redundant resources.

The Good

Cloud computing



Specialist
Staff

Uniform
Platform

Concentration

Availability
and Access

Recovery

The Good

Cloud computing



Many advantages also have many limitations and present problems ...

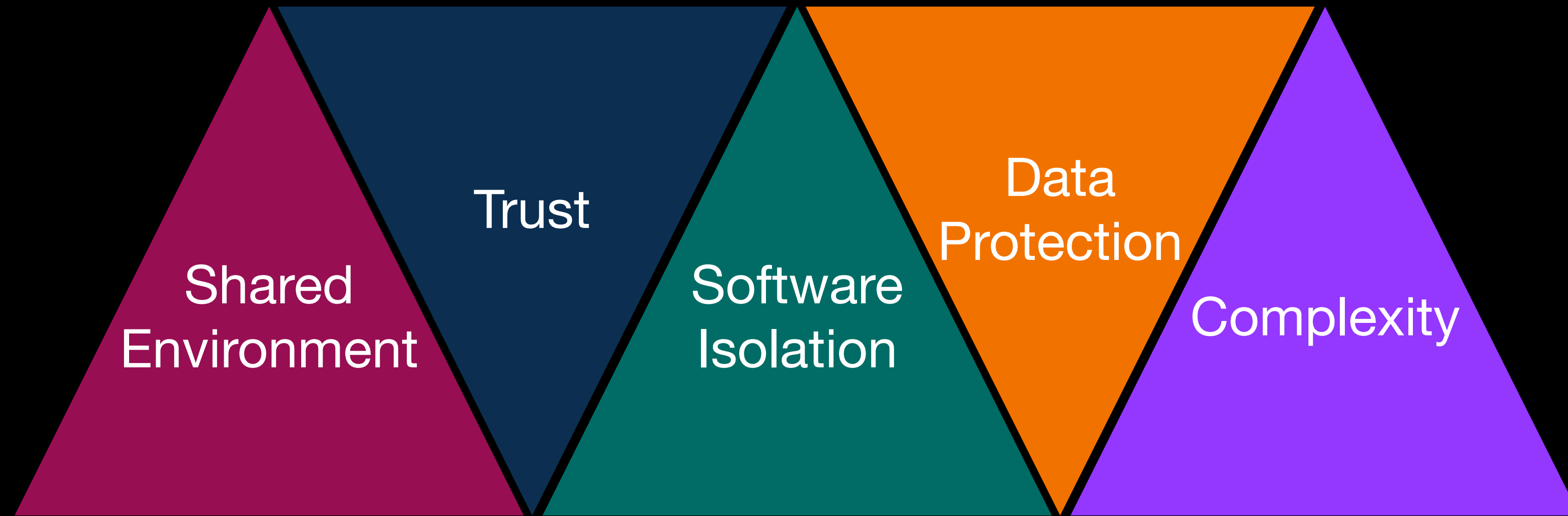
The Good,
the Bad
and the Ugly.

The Good,
the Bad
and the Ugly.

The Good,
the Bad
and the Ugly.

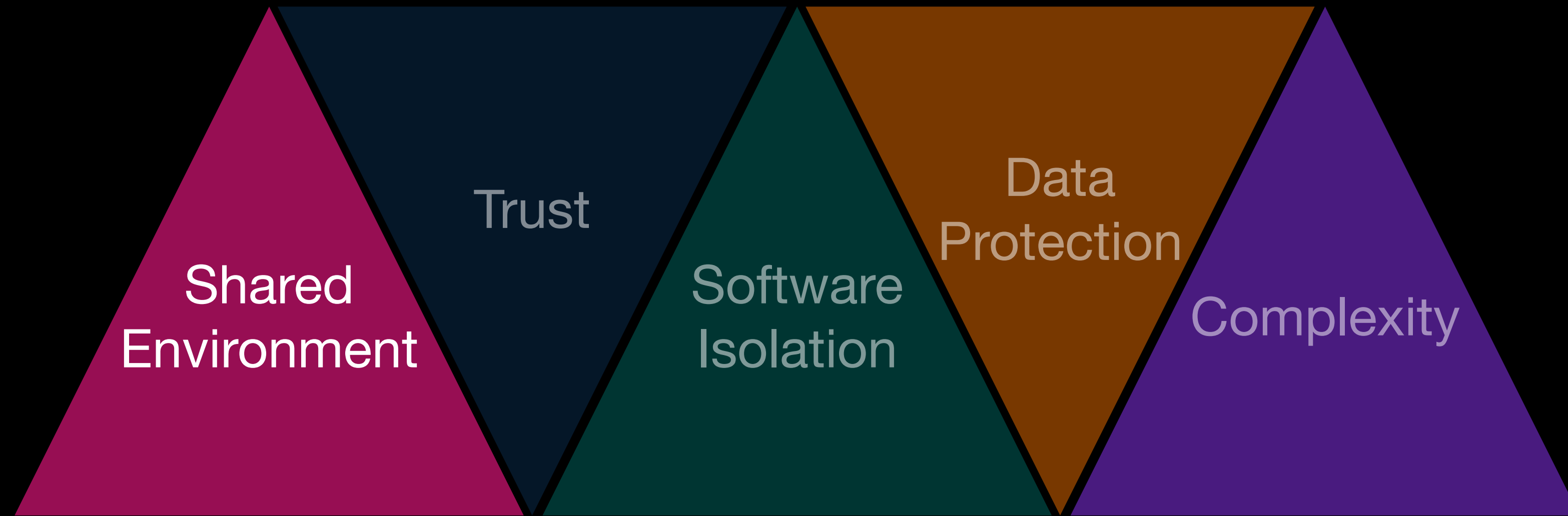
The Bad

Cloud Computing



The Bad

Cloud Computing



The Bad

Cloud Computing

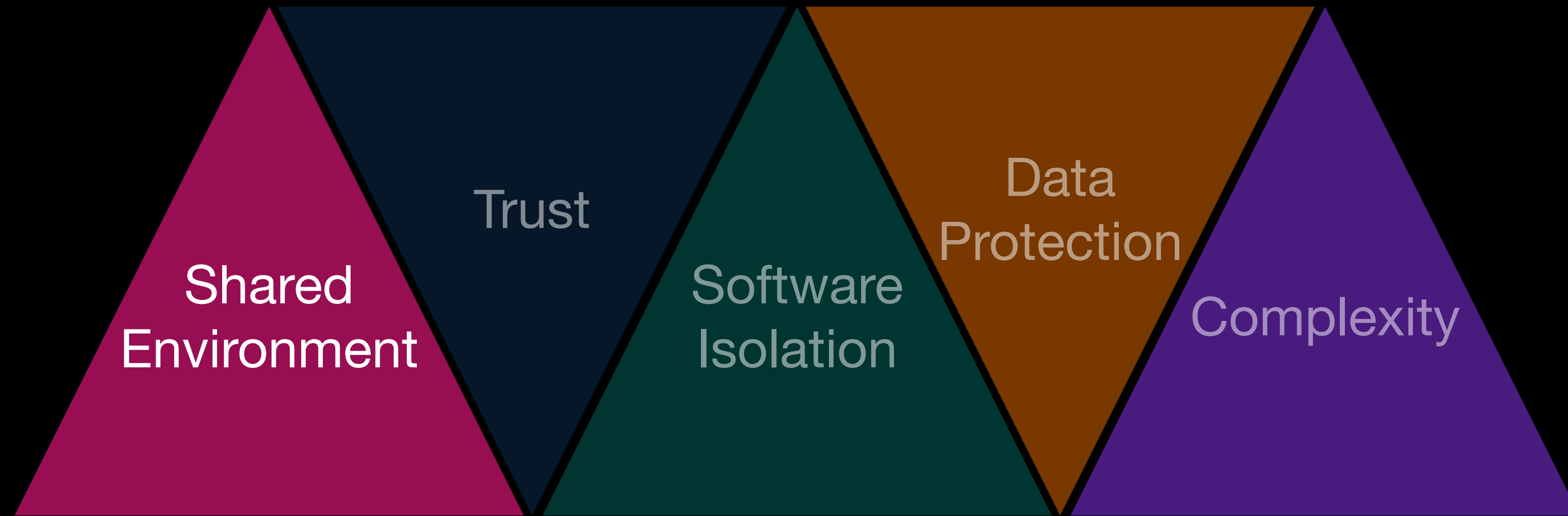


Shared
Environment

- **Depending on deployment**, clients share elements of the infrastructure.
- Rather than physical separation, **logical separation** of resources is utilised that can be exploited by malicious attackers.
- **Non-malicious actions**, such as software or configuration error, could also hamper access and communication across components.
- Multi-tenant environments require **significant assurances around security** that ensure logical separation.

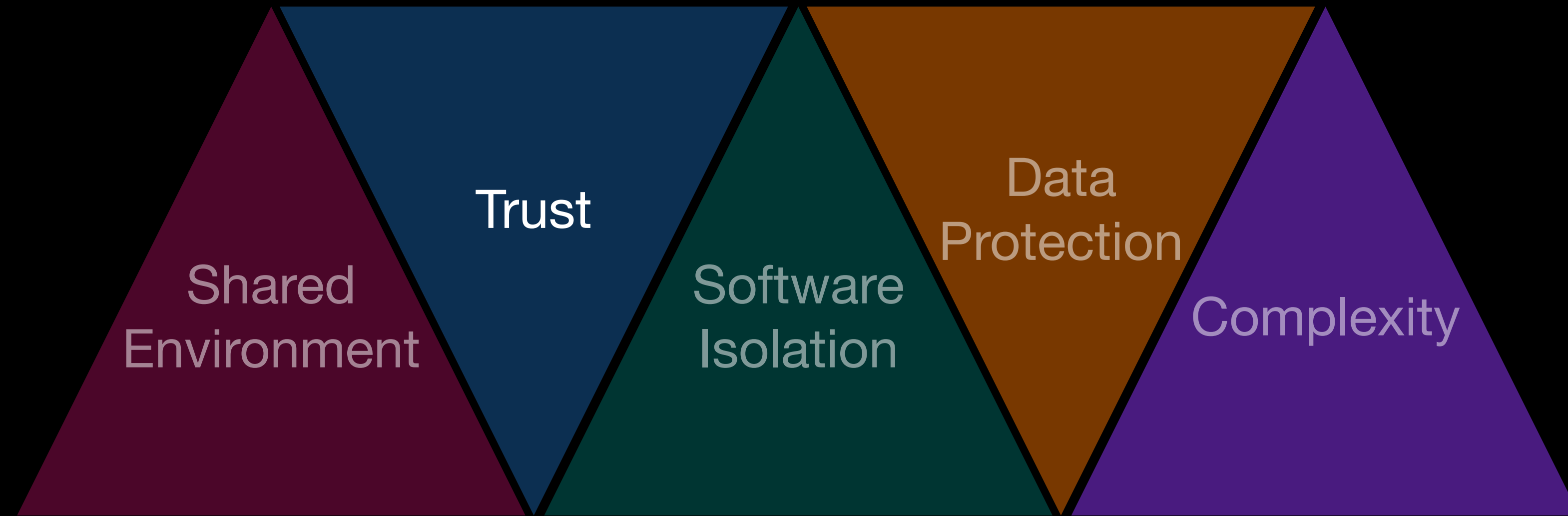
The Bad

Cloud Computing



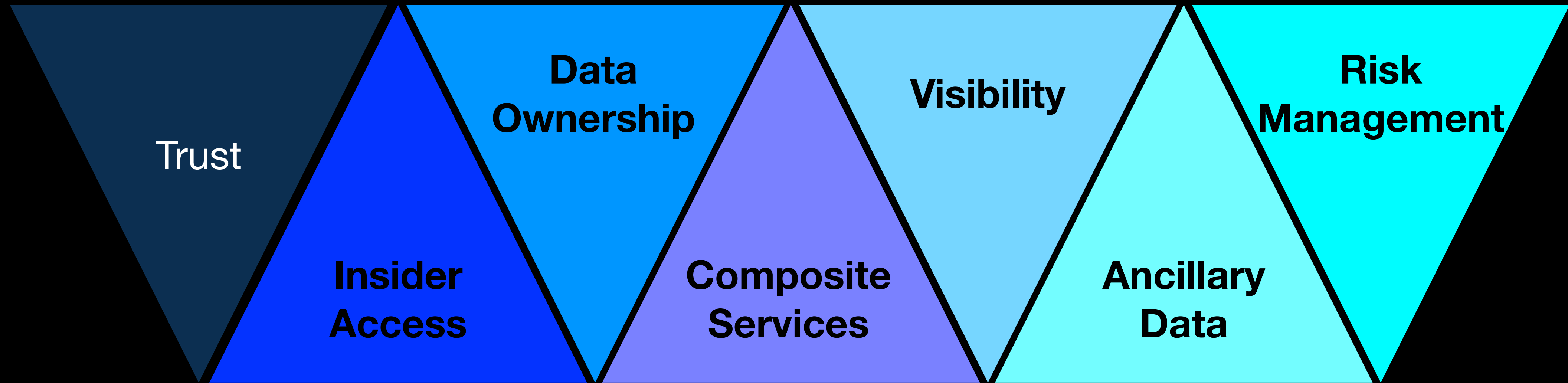
The Bad

Cloud Computing



The Bad

Cloud Computing



The Bad

Cloud Computing

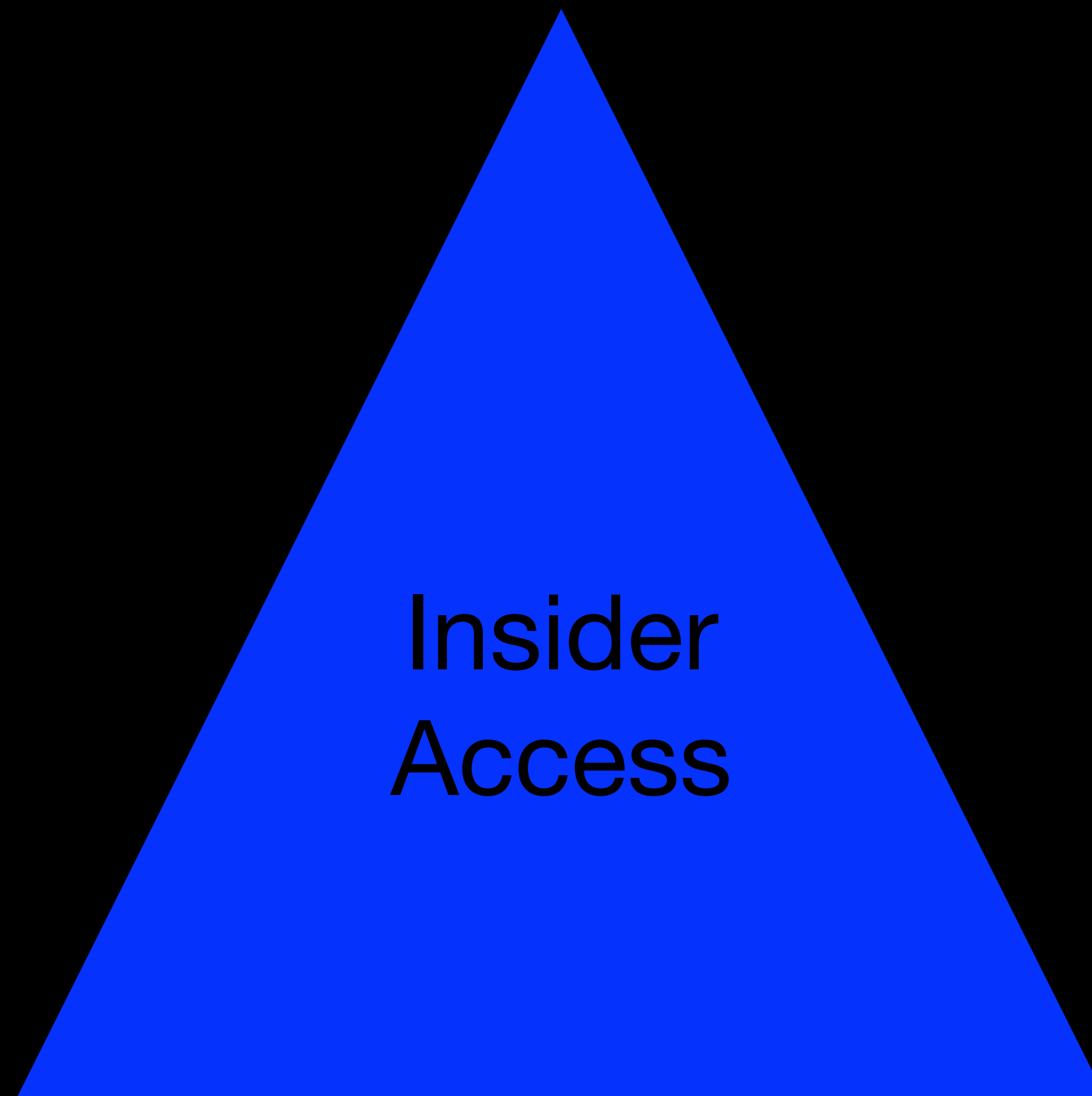


Trust

- Enterprises are relying on cloud providers for infrastructure and for aspects of security and privacy.
- States and Governments have to protect their people, both in terms of infrastructure collapsing and/or being disrupted as well as information being disclosed, destroyed or modified.
- Enterprises and Cloud Providers need to operate with a high-level trust.

The Bad

Cloud Computing



- **Insider threats** is a serious and common threat for most organisations, including cloud providers and enterprises.
- Cloud computing expands the number of potential malicious insiders as well as the level of threat.
- Cloud providers and enterprises need to consider and address the threat of insiders within their given context.

The Bad

Cloud Computing



Data
Ownership

- Cloud providers and enterprises need to ensure clarity the ownership of data, both in terms of each other and their clients.
- For example it must be clear the owner of data in terms of the enterprise and cloud provider as well as their users.
- Contracts and terms of services must be clear between all parities.

The Bad

Cloud Computing



Composite
Services

- Different offerings from cloud providers can utilise the infrastructure of other cloud providers, for SaaS offering using IaaS from another provider.
- Cloud providers could also outsource or subcontract their activities to other cloud providers or entities.
- Responsibility for failure as well as data must be established between parties.
- Regulations in different jurisdictions govern aspects of outsourcing and subcontracting.

The Bad

Cloud Computing

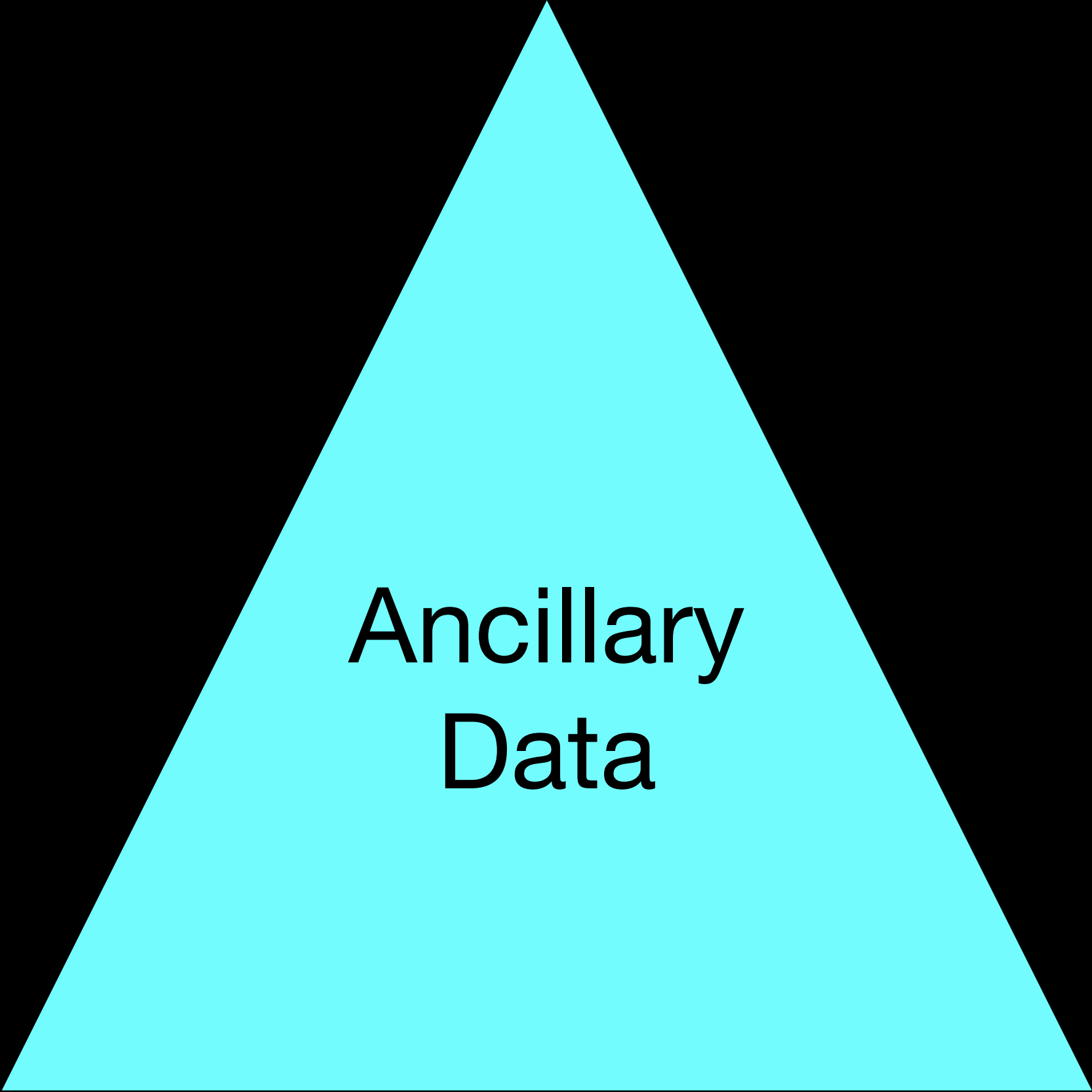


Visibility

- Continuous monitoring of infrastructure is invaluable in mitigating the risk of flawed configuration or poor security controls.
- Enterprises need to know the security strategy and policy of cloud providers to properly evaluate risk.
- Transparency in operations (including composite arrangements) is necessary to properly govern security and privacy.

The Bad

Cloud Computing



Ancillary
Data

- Cloud providers can be responsible for personal data and sensitive data.
- Data such as payment information or emails addresses could be compromised in breaches that could result in subsequent attacks.
- Cloud providers also collect data about enterprises and use of services, for example measured service data.

The Bad

Cloud Computing

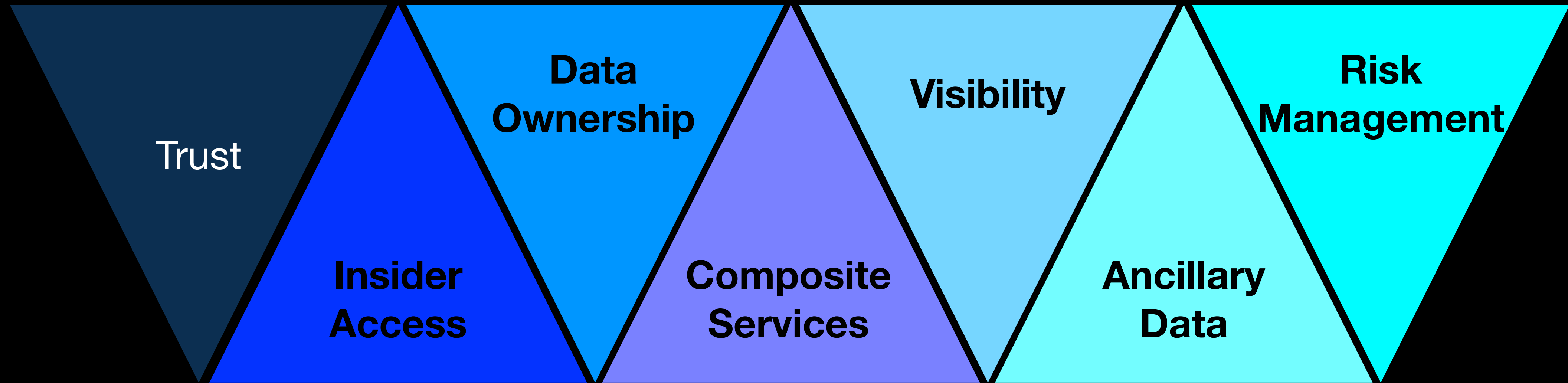


Risk
Management

- Risk can be difficult for enterprises to manage when it falls outwit their perimeter.
- Regulations or agreements could require specific security controls that are realistically beyond the control of the organisation.
- Trust is central to risk management as if an organisation is not able to trust partners it either has to not engage them or accept higher risk.

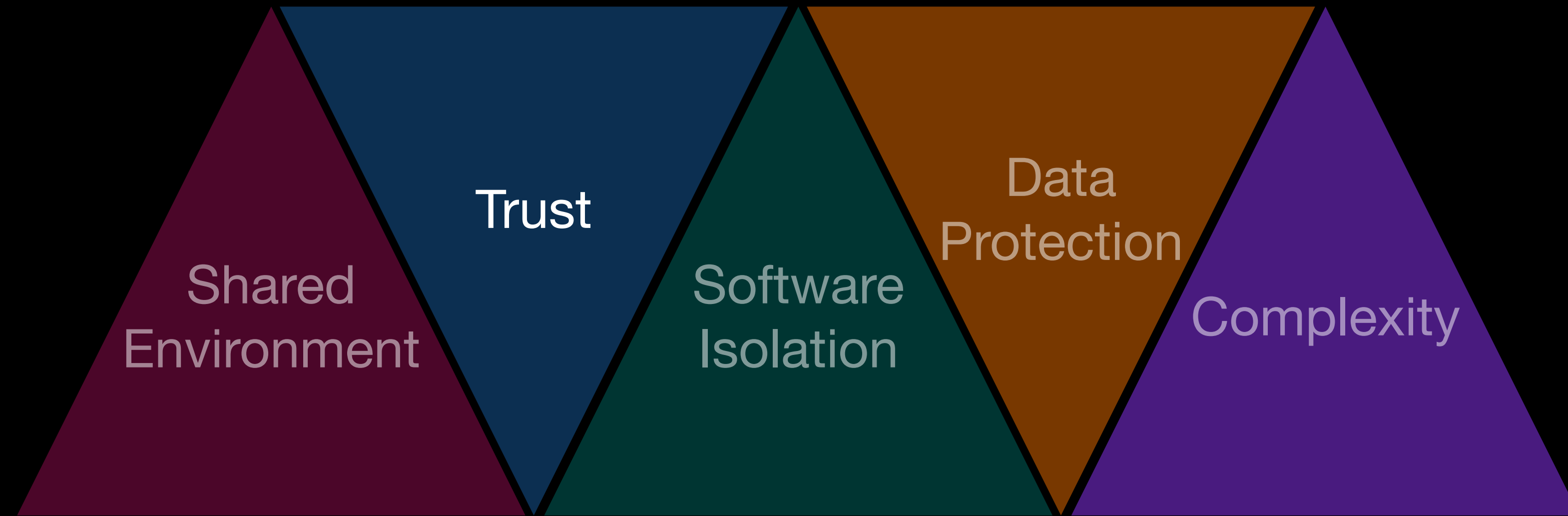
The Bad

Cloud Computing



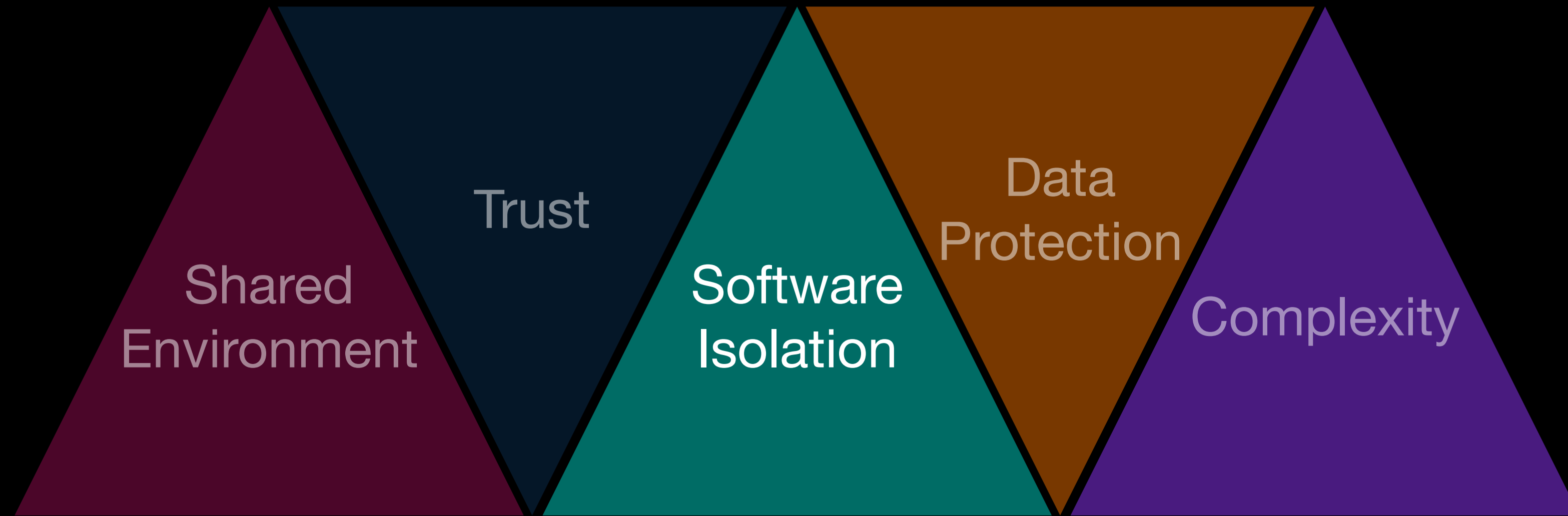
The Bad

Cloud Computing



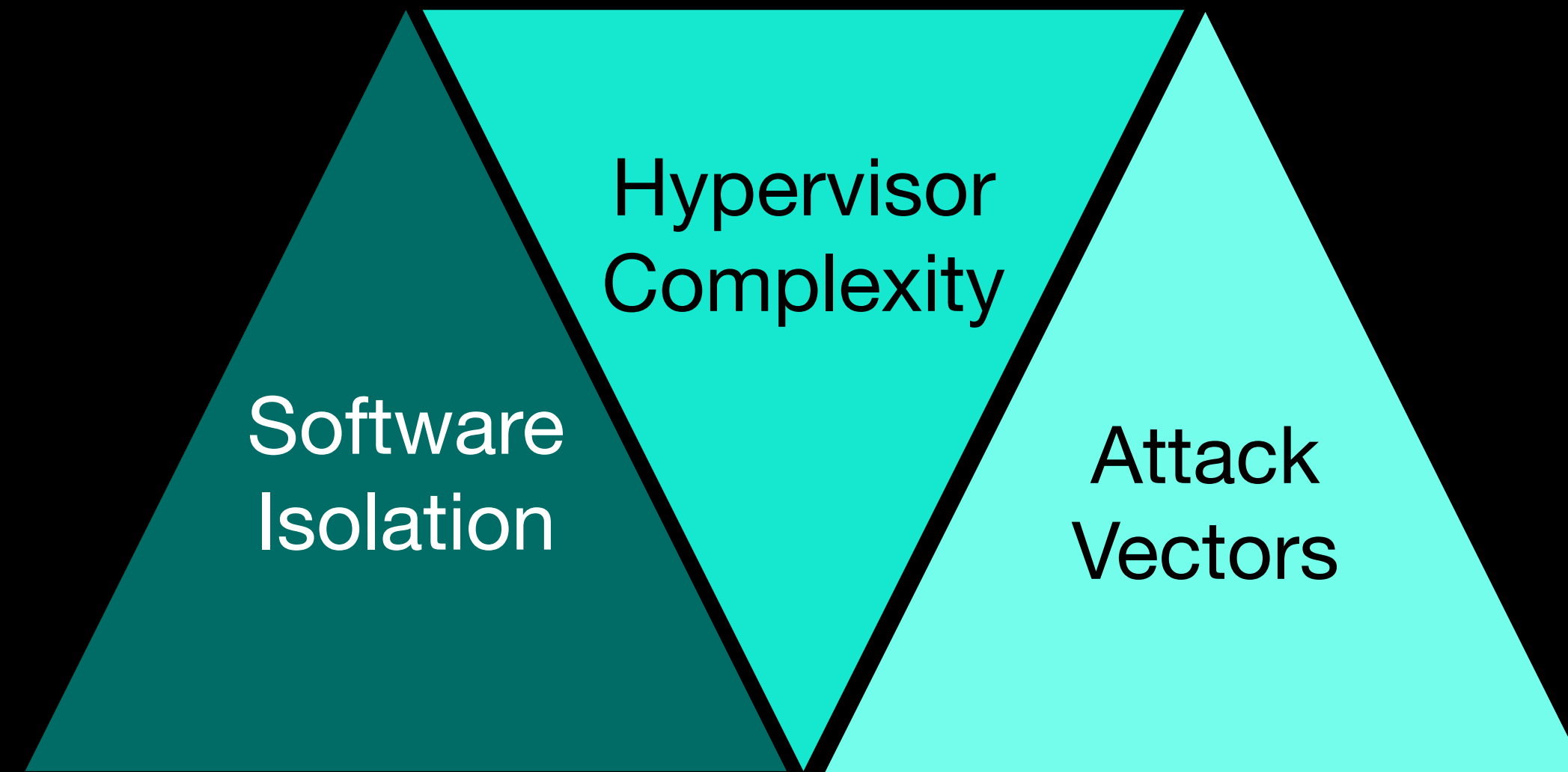
The Bad

Cloud Computing



The Bad

Cloud Computing



The Bad

Cloud Computing



Software
Isolation

- Multi-tenancy is required to achieve the envisioned benefits of cloud computing.
- Different approaches can be used to managing multi-tenancy, but this is complex.

The Bad

Cloud Computing



Hypervisor
Complexity

- Hypervisor is central to ensuring the logical separation between virtual elements in cloud providers between tenants.
- Hypervisors can be small and compact and can consequently be vetted and analysed to ensure strong separation.
- In reality, hypervisors are often large and complex and can be extremely difficult to analyse and mitigating against security risk.

The Bad

Cloud Computing

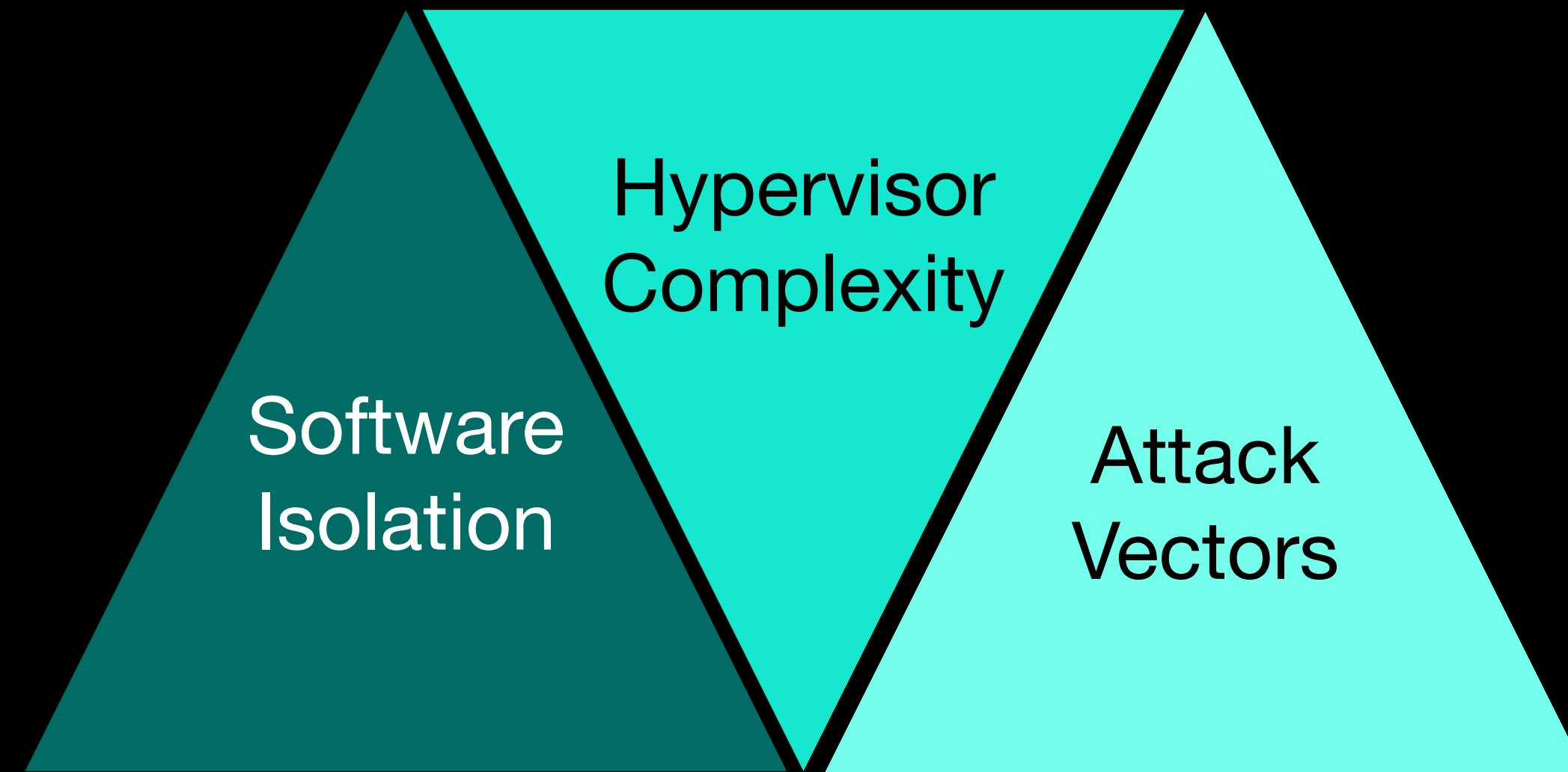


Attack
Vectors

- Malicious code can escape some virtual machines and compromise the hypervisor or other virtual machines.
- Endpoints for engineers as well as clients can act as entry points for attackers.
- Dashboards used by enterprises to manage and monitor cloud computing access can also common entry points.

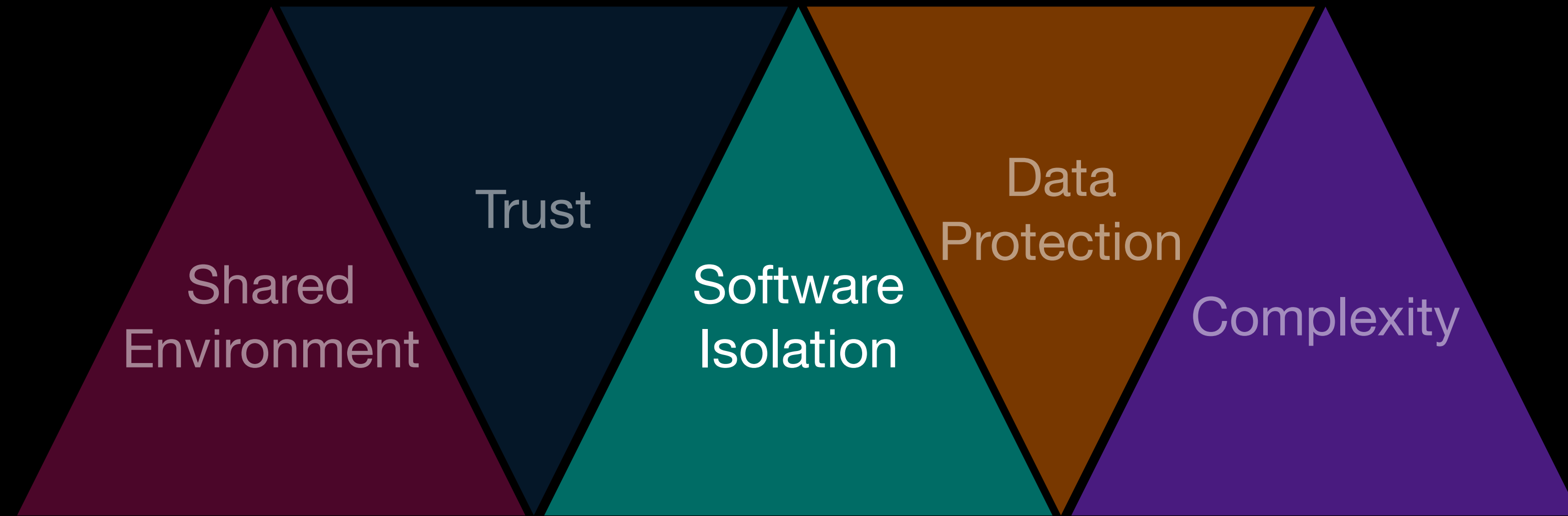
The Bad

Cloud Computing



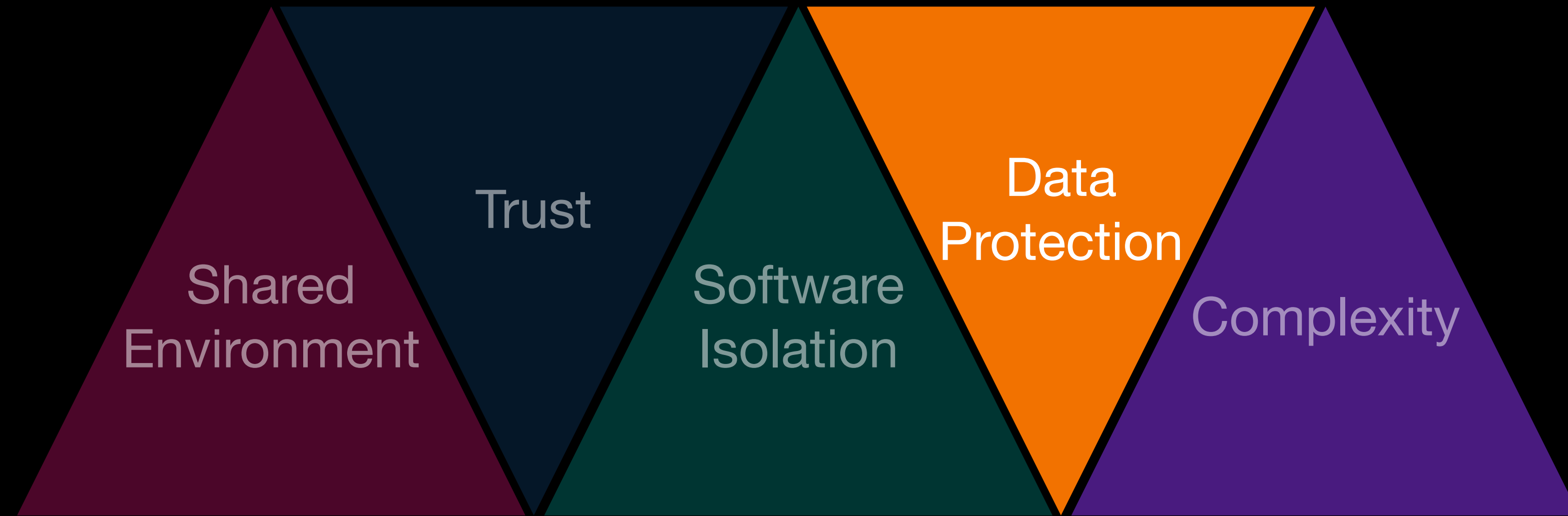
The Bad

Cloud Computing



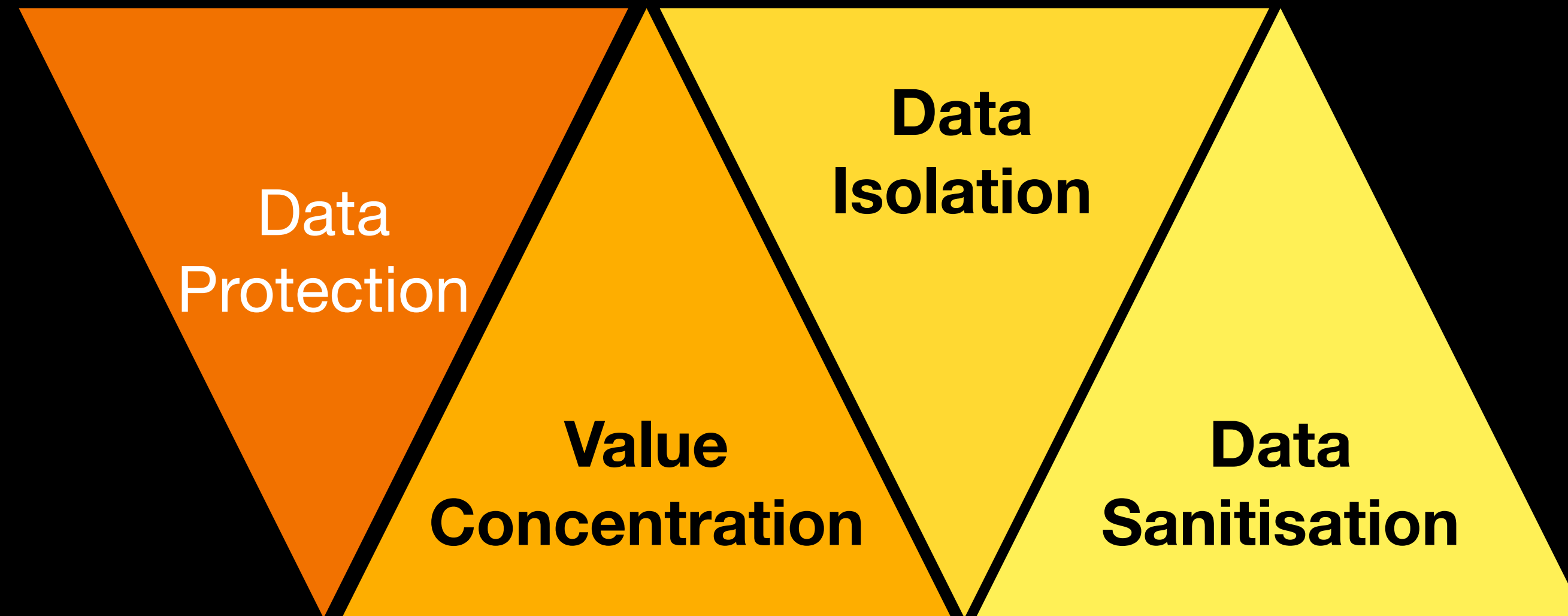
The Bad

Cloud Computing



The Bad

Cloud Computing



The Bad

Cloud Computing



Value
concentration

- Data can prove a valuable entity in the modern economy and this can motivate malicious actors to target cloud providers to gain access to data.
- Loss or disruption of data and/or services may also provide desirable due to the impact caused from the loss of service, for example data associated with health or finance.

The Bad

Cloud Computing



Data
Isolation

- Data needs to be protected while it is in use, in transit between elements and while at rest.
- Encryption is often the key tool in maintaining the security of data.
- Architecture of cloud provider infrastructure also has to be considered to ensure data is not unintentionally mixed with other data.

The Bad

Cloud Computing

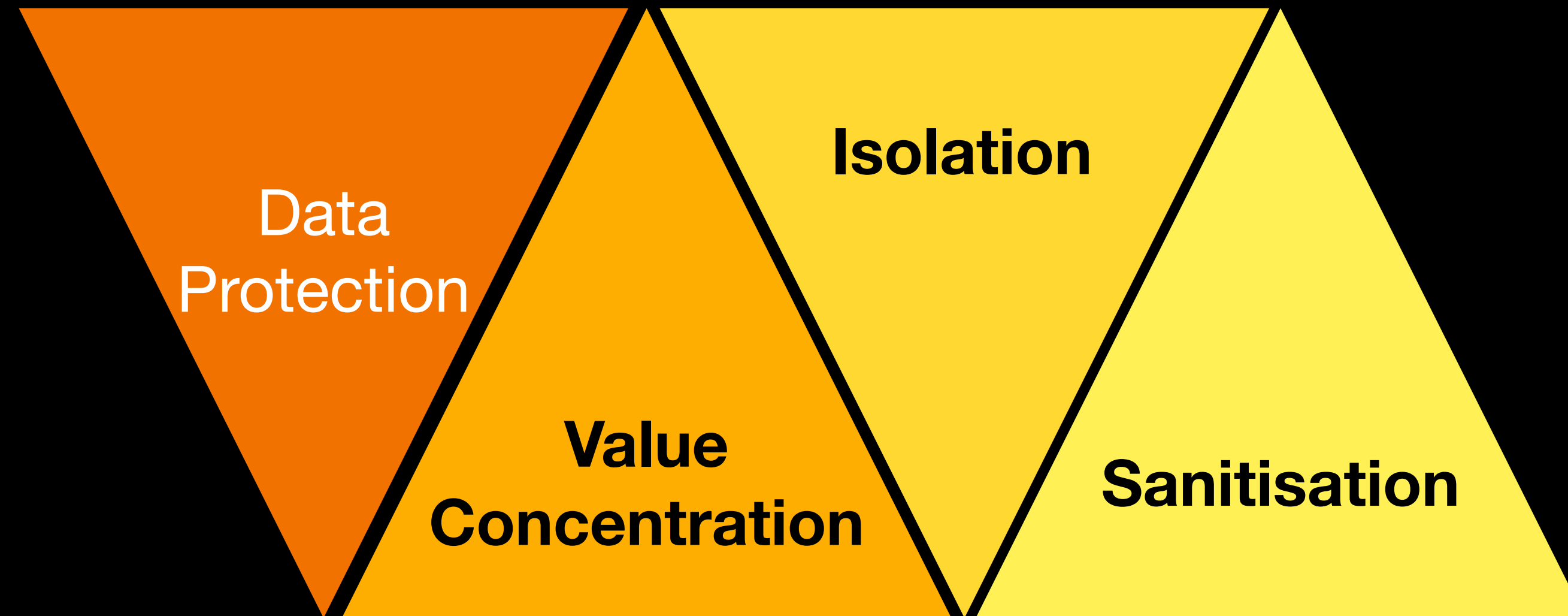


Data
Sanitisation

- Data is often mixed or colocated with other client data.
- Data can also be propagated across different infrastructures for various reasons, for example subcontracting of services or back-up.
- Regulations guide data beyond use, but also have to consider replacement of components within cloud provider infrastructure.

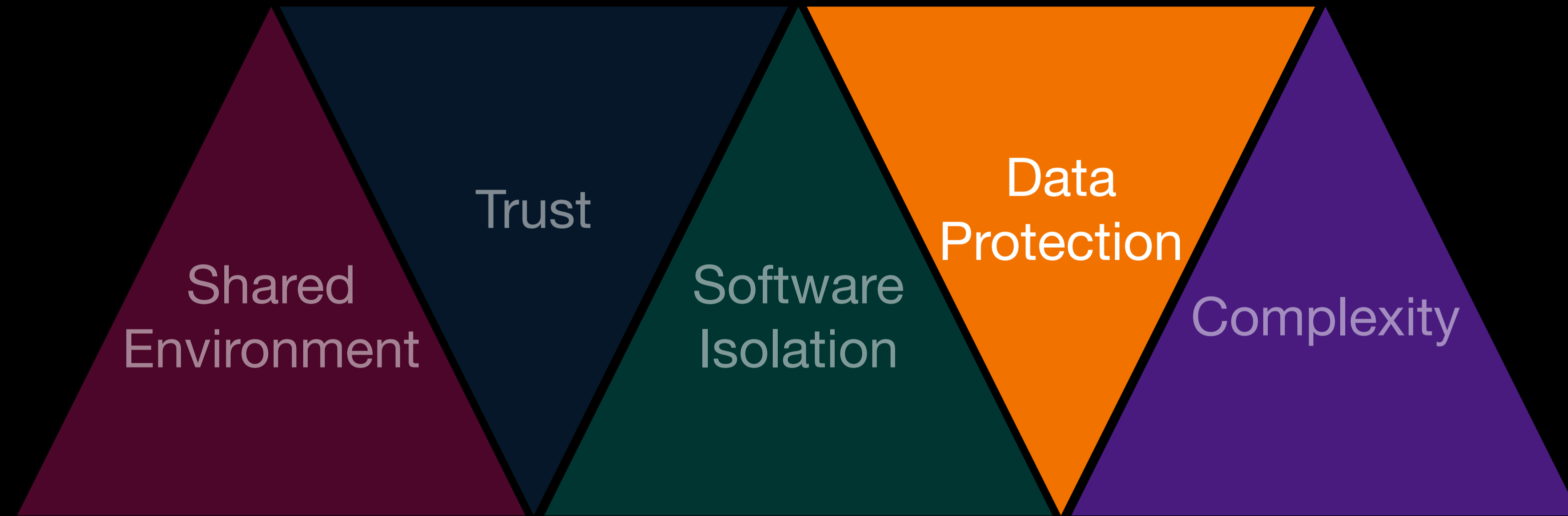
The Bad

Cloud Computing



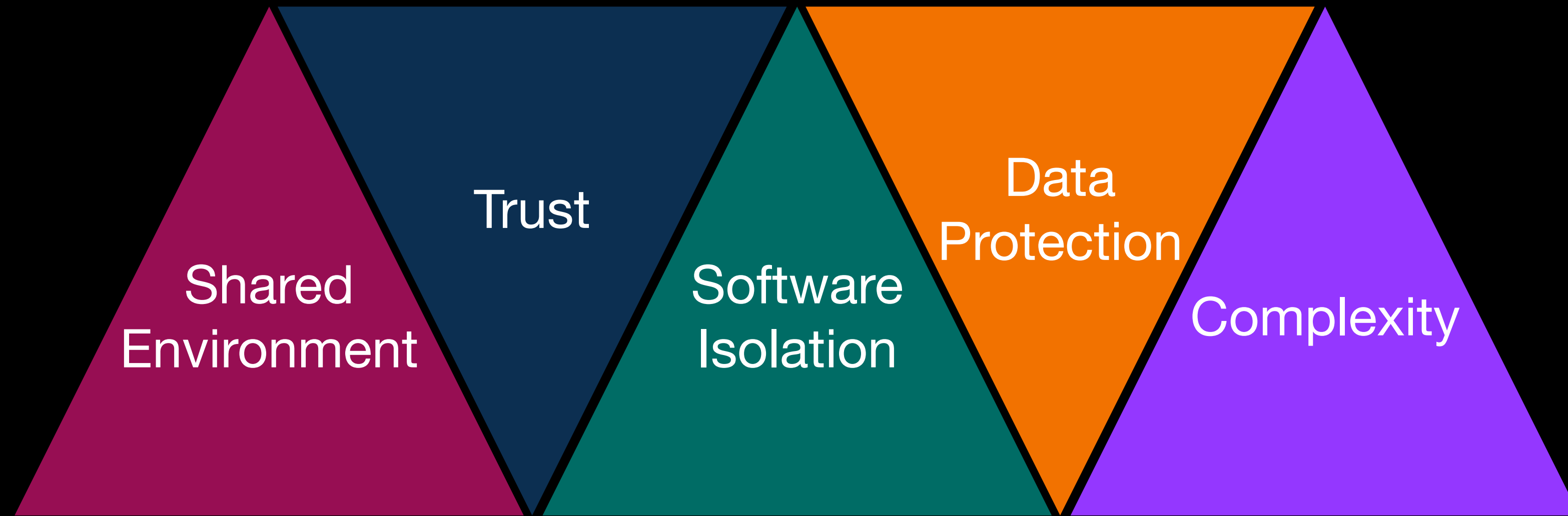
The Bad

Cloud Computing



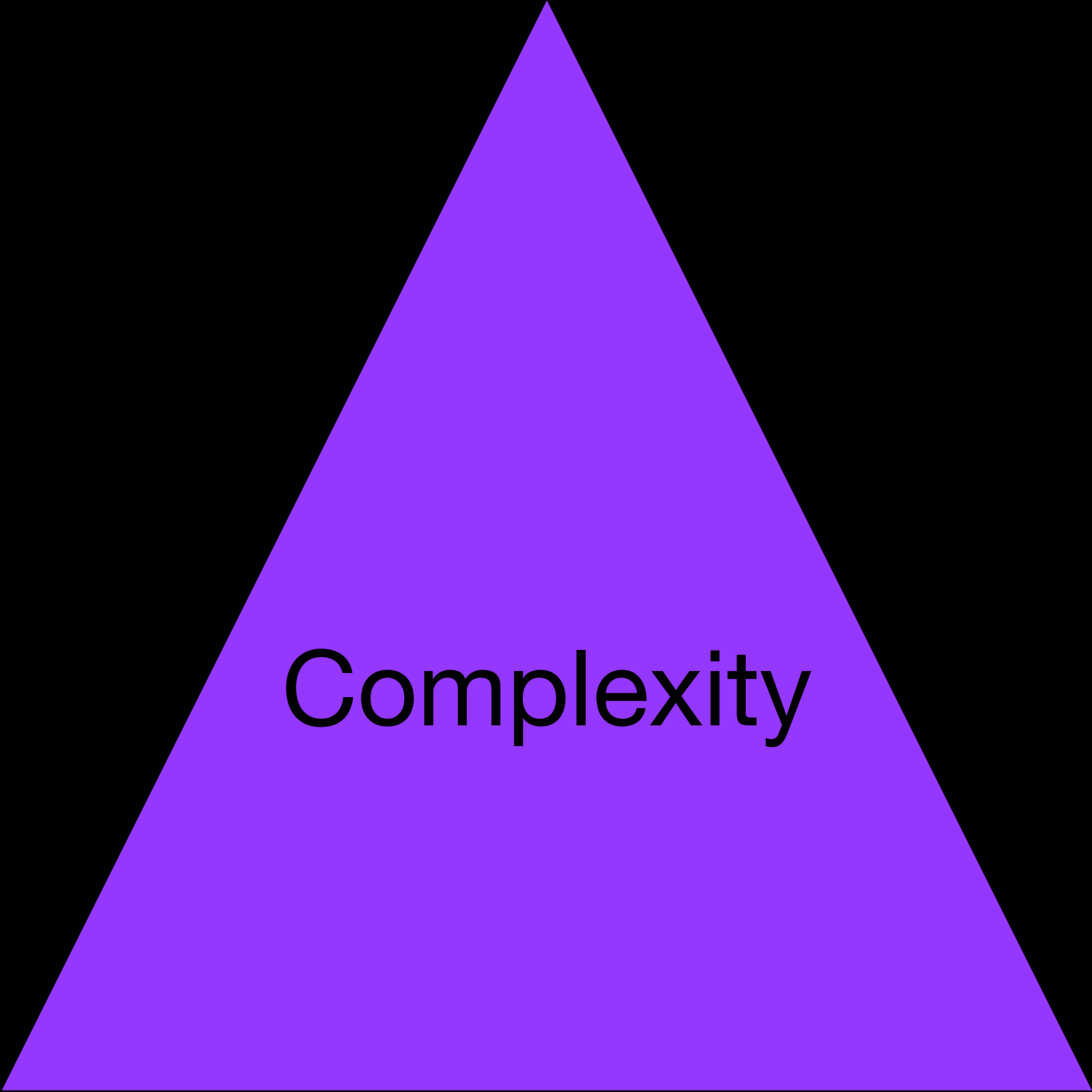
The Bad

Cloud Computing



The Bad

Cloud Computing



Complexity

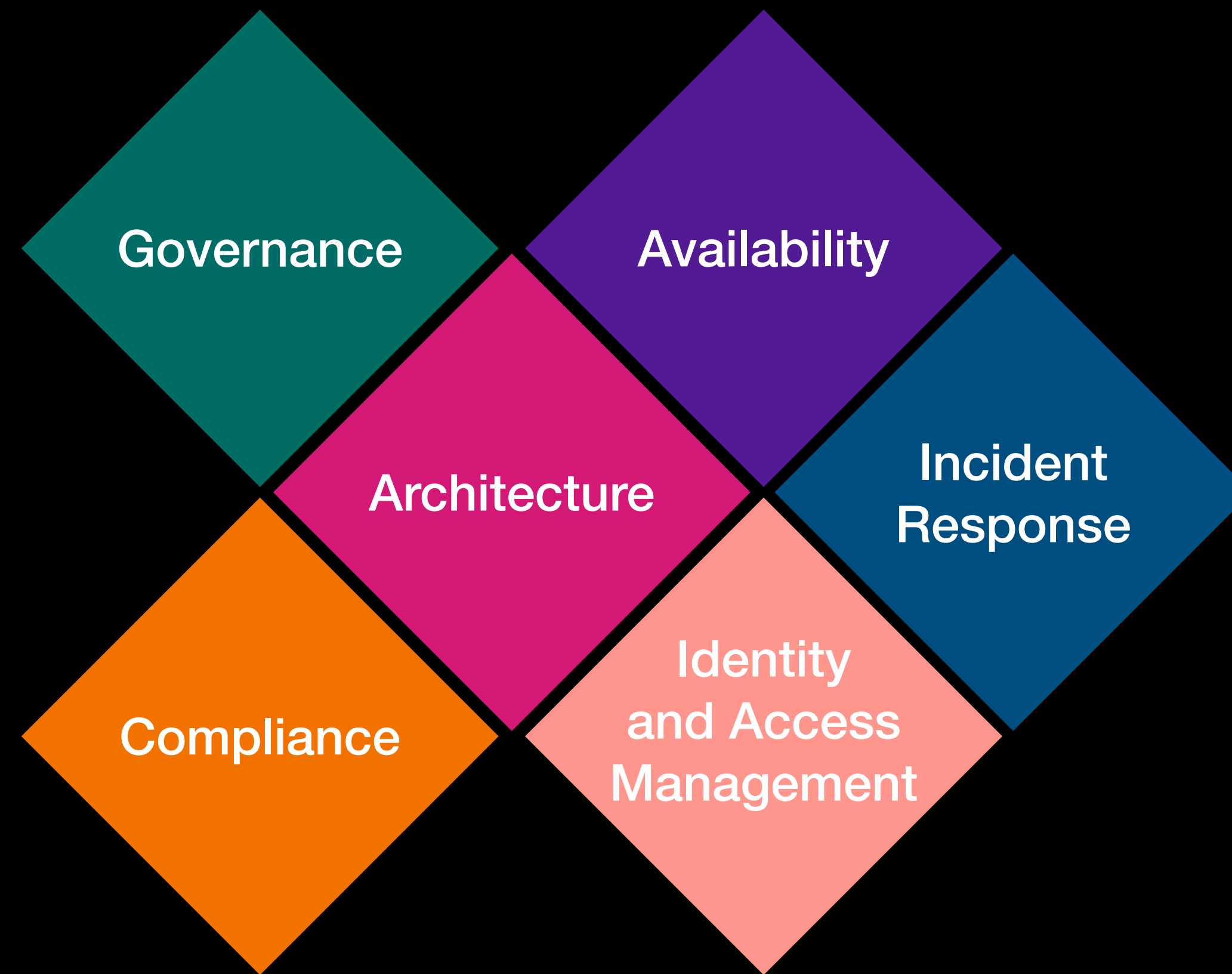
- Complexity of cloud providers makes it incredibly challenging to meet security and privacy requirements for enterprises.
- Enterprise must plan to transition to cloud computing infrastructure and must have insight into the cloud providers.

The Good,
the Bad
and the Ugly.

The Good,
the Bad
and the Ugly.

The Ugly

Cloud Computing



The Ugly

Cloud Computing



The Ugly

Cloud Computing

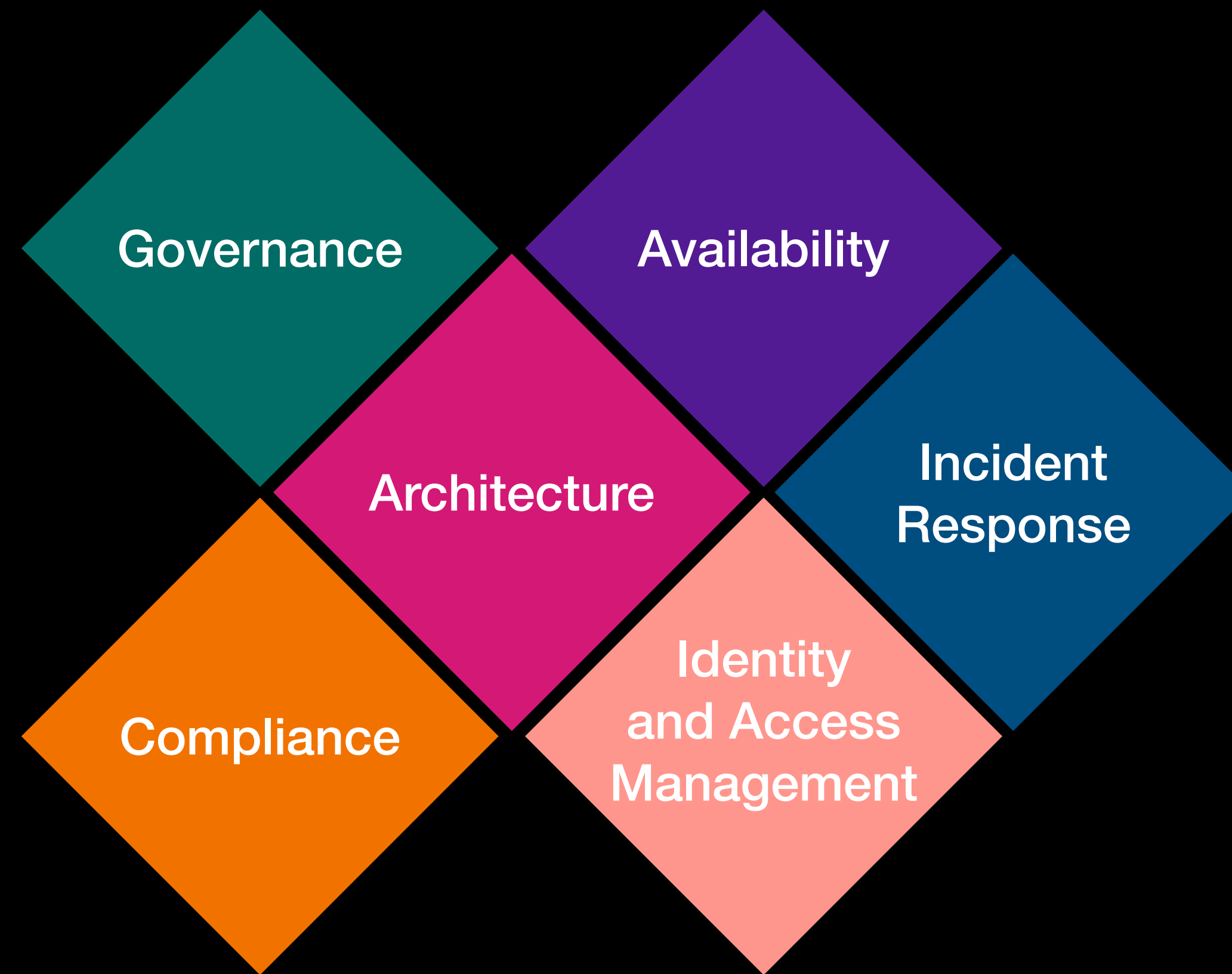


Governance

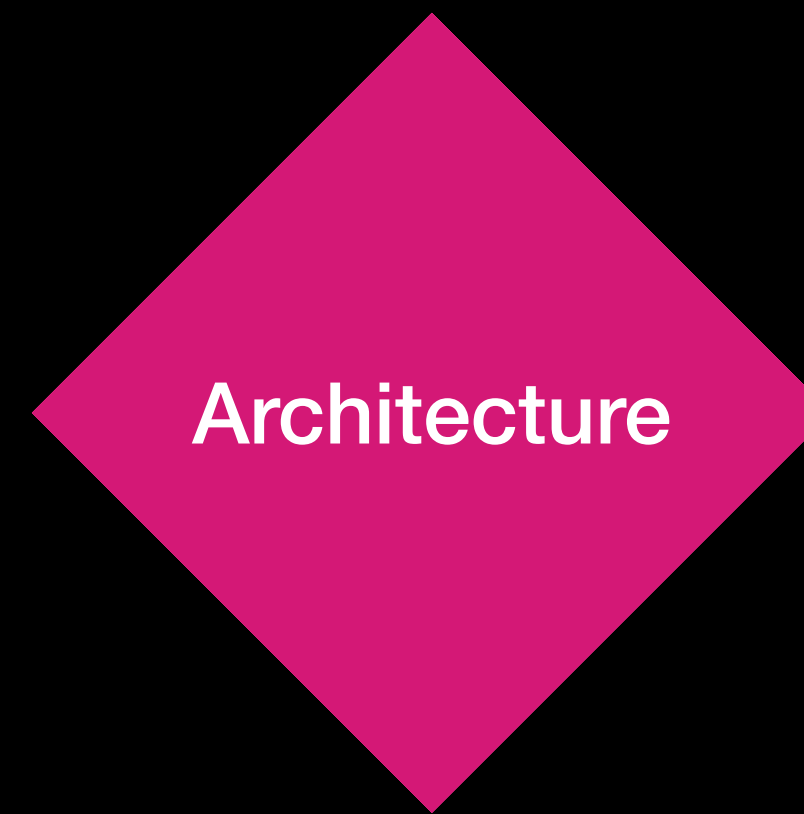
- Cloud computing availability ensures the companies **can access resources rapidly and benefits from expenditure quickly.**
- Concern is that governance is weakened as elements with enterprises can engage cloud computing infrastructure.
- Result is complex mess of cloud computing interactions with limited governance.

The Ugly

Cloud Computing

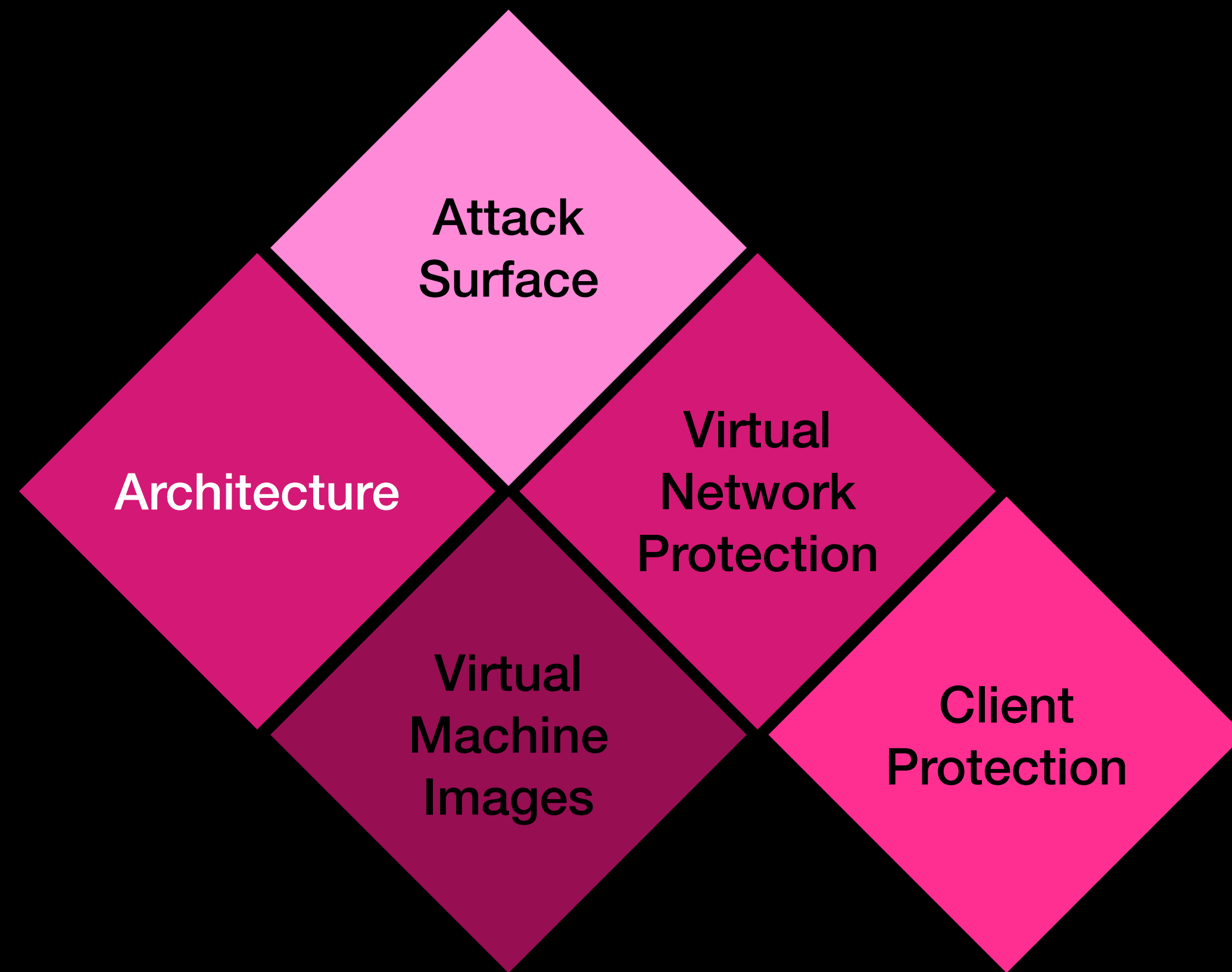


The Ugly Cloud Computing



The Ugly

Cloud Computing



The Ugly

Cloud Computing



Architecture

- Architecture of the cloud provider depends on the provider, location and offering.
- The client or enterprise in terms of their hardware and software as well as how it is protected it also important to consider.

The Ugly

Cloud Computing



Attack Surface

- Hypervisors used by cloud providers introduce significant complexity when contrasted with traditional operating systems on single systems.
- The complexity can provide more opportunities for attackers to compromise infrastructure.

The Ugly

Cloud Computing



Virtual Machine Images

- Sharing images of virtual machines between providers to support efficient and effective generation of virtual machines is common.
- Moreover, common for enterprises to maintain libraries of virtual machines images.
- Important to ensure these are properly configured and analysed to minimise entry points for attackers.

The Ugly

Cloud Computing



Virtual Network Protection

- Virtual network switches and configurations afford more efficient communication between virtual elements within cloud infrastructure.
- Virtual network elements may lack the same visibility as physical network infrastructure and may not be recognised by monitoring solutions designed for physical network elements.

The Ugly

Cloud Computing

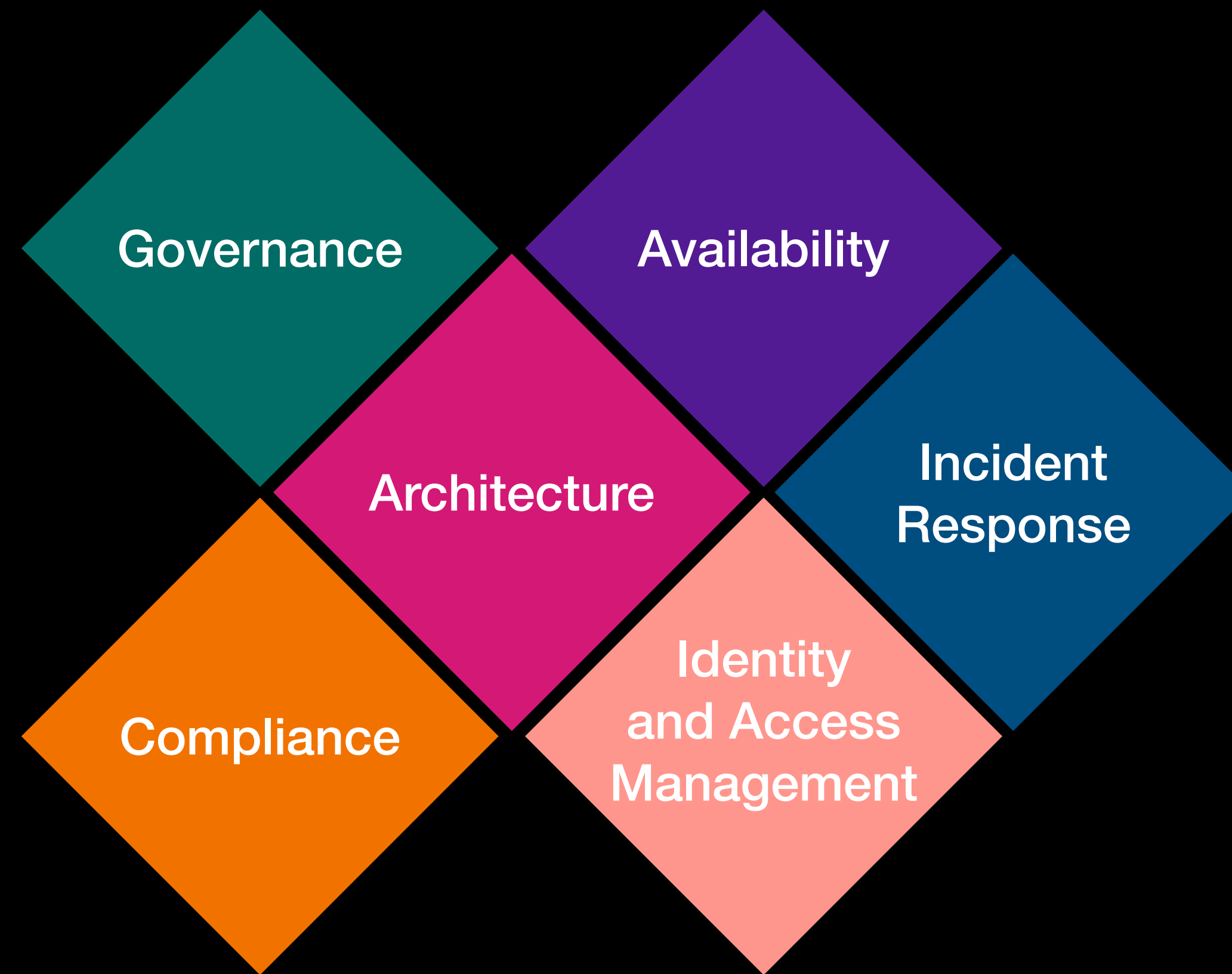


**Client
Protection**

- Easy for enterprises to neglected consideration on-premise security as they outsource more of their infrastructure to cloud providers.
- Enterprises must ensure they manage the security and privacy of the endpoints within the organisation.

The Ugly

Cloud Computing



The Ugly

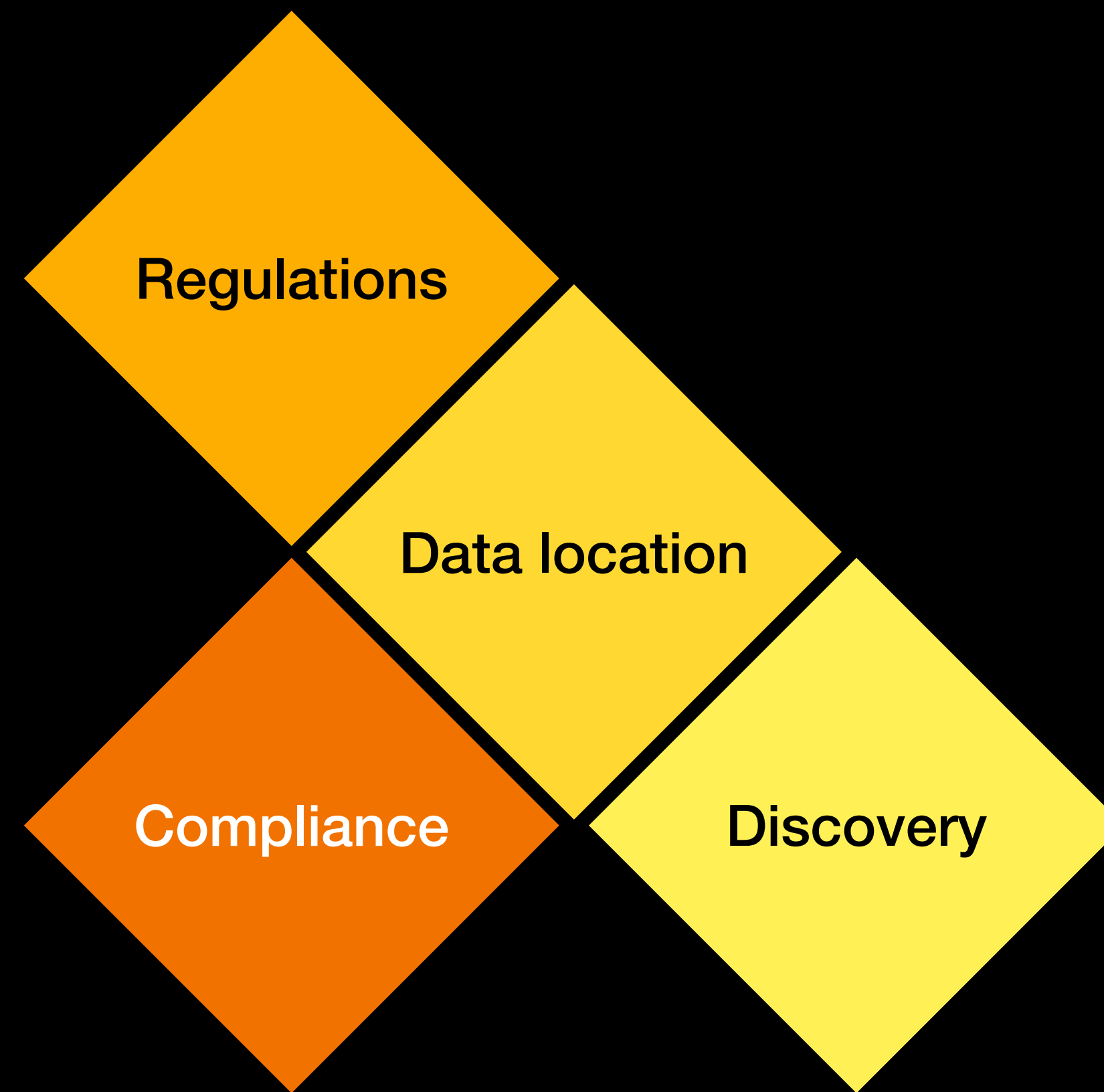
Cloud Computing



Compliance

The Ugly

Cloud Computing



The Ugly

Cloud Computing



Compliance

- Compliance is the ability of an organisation to operate within the limits of laws, standards and regulations.
- Many territories around the world have various laws and regulations as well as numerous organisations have numerous policies and specifications.

The Ugly

Cloud Computing



Regulations

- There are numerous laws in the European and American context that regulate systems as well as data.
- General Data Protection Regulations is important in the European context, various acts in the United States as well as industry relevant acts and specifications.
- For example Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI DSS).

The Ugly

Cloud Computing



Data Location

- Data location is a significant compliance issue for companies and cloud providers.
- Specifically data at rest as well as transborder data flows.
- There are also less obvious regulations that are difficult for companies to confirm, for example requirement for data records to stored at specific heights and distances from disaster zones.

The Ugly

Cloud Computing

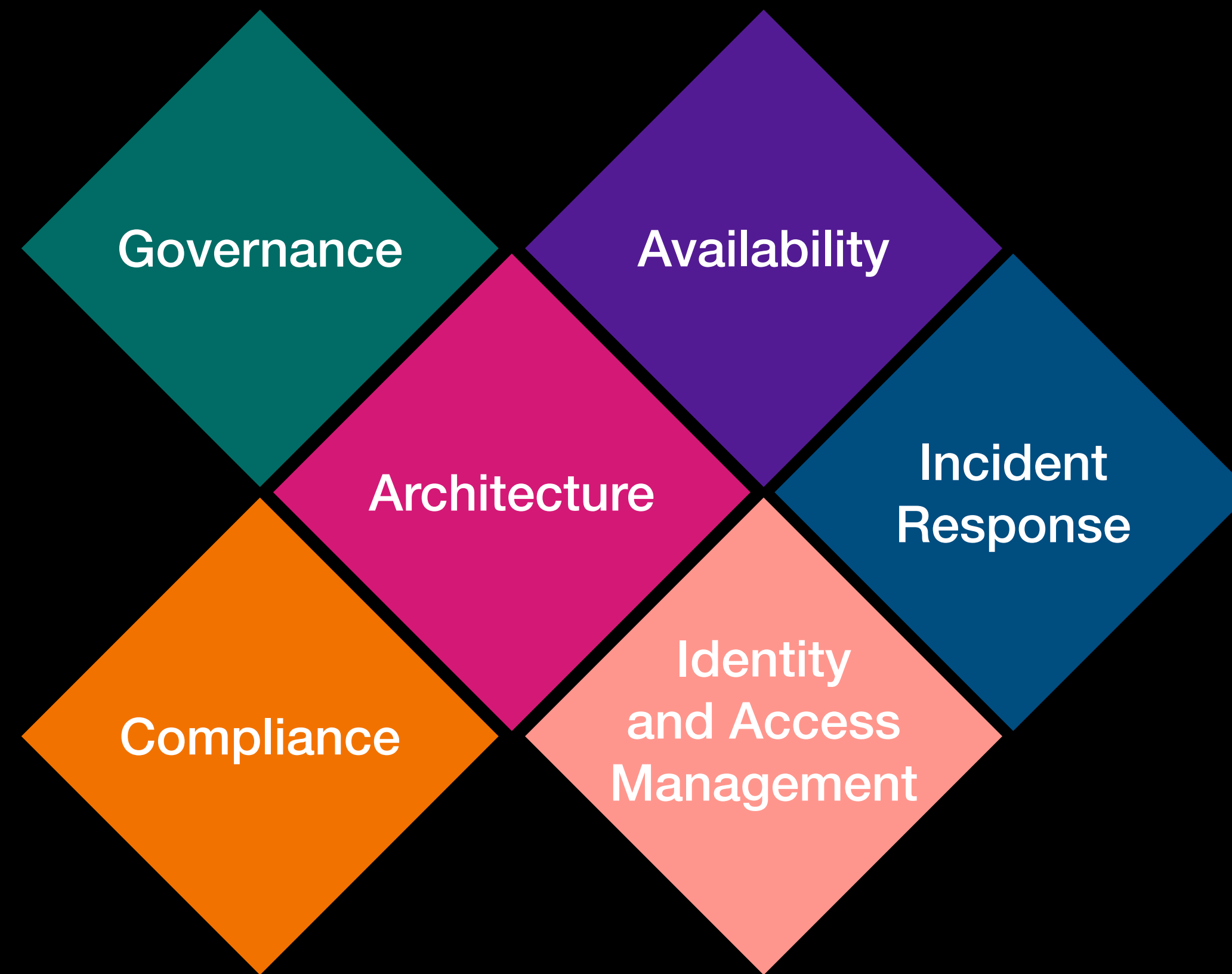


Discovery

- Electronic discovery for legal cases as well as fulfilling other acts if a critical issue for cloud providers and organisations. For example, the Freedom of Information Act (FoIA) as well as litigation.
- Cloud providers may not have tools that support requests within a given jurisdiction or meet requirements, for example sufficient meta-data.

The Ugly

Cloud Computing



The Ugly

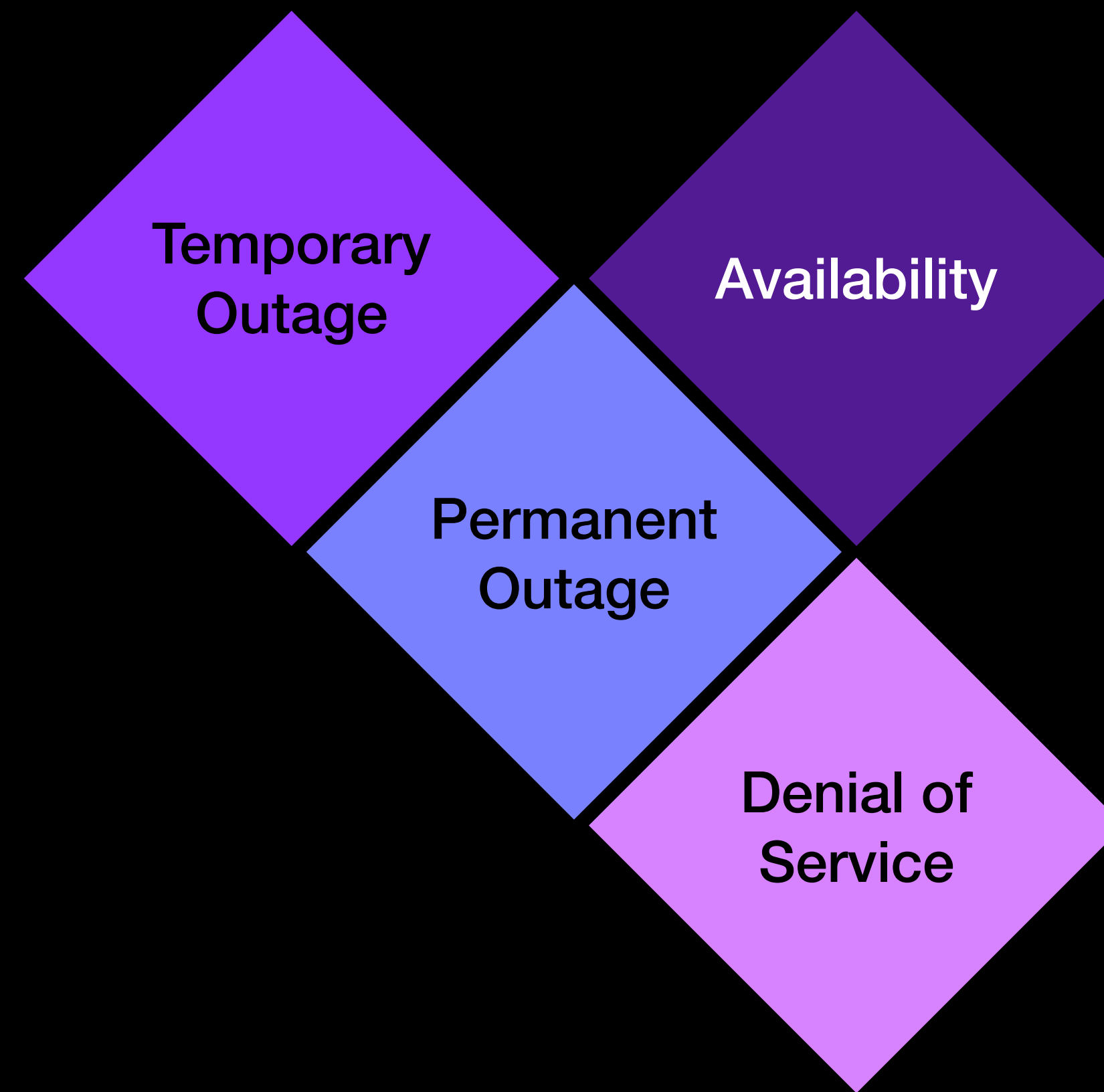
Cloud Computing



Availability

The Ugly

Cloud Computing



The Ugly

Cloud Computing



Availability

- Availability refers to the ability of the enterprise to access services and data.
- Availability of cloud computing resources could be temporary or permanently impacted.
- The risk to typical mitigate against is unplanned downtime as this can impact on the goals of the organisation.

The Ugly

Cloud Computing

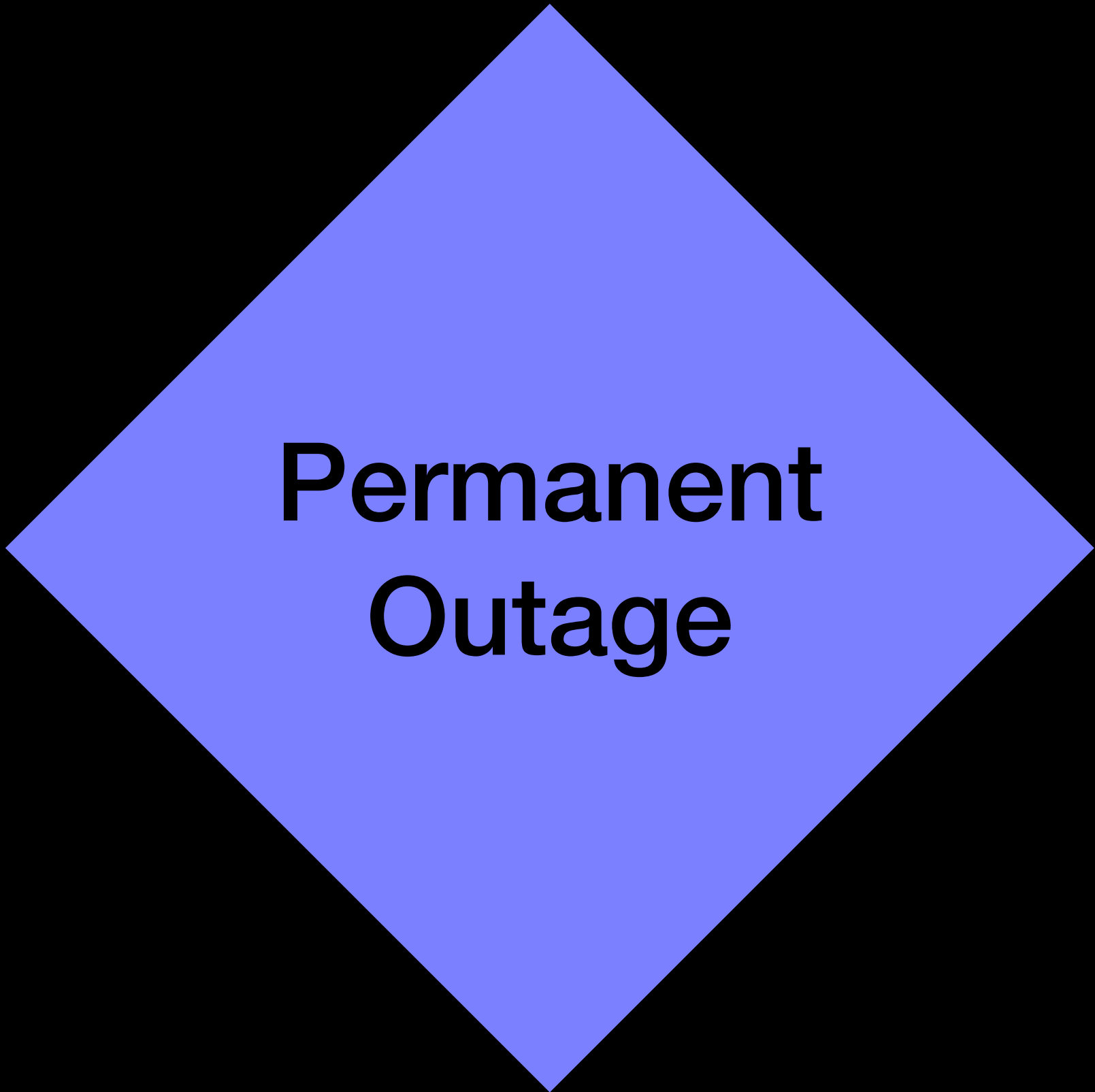


**Temporary
Outage**

- Temporary outage could result in infrastructure not be available to hours, depending when this temporary outage happens this can have significant impacts on organisations.
- Service Level Agreements (SLAs) can be used to ensure cloud providers comply with the expectations and requirements of enterprises.

The Ugly

Cloud Computing



**Permanent
Outage**

- Enterprises need to consider contingency plans for permanent outages.
- Cloud providers can become bankrupt or may depart different jurisdictions for various reasons.
- Cloud providers can also be required to cease operations due to legal concerns.

The Ugly

Cloud Computing

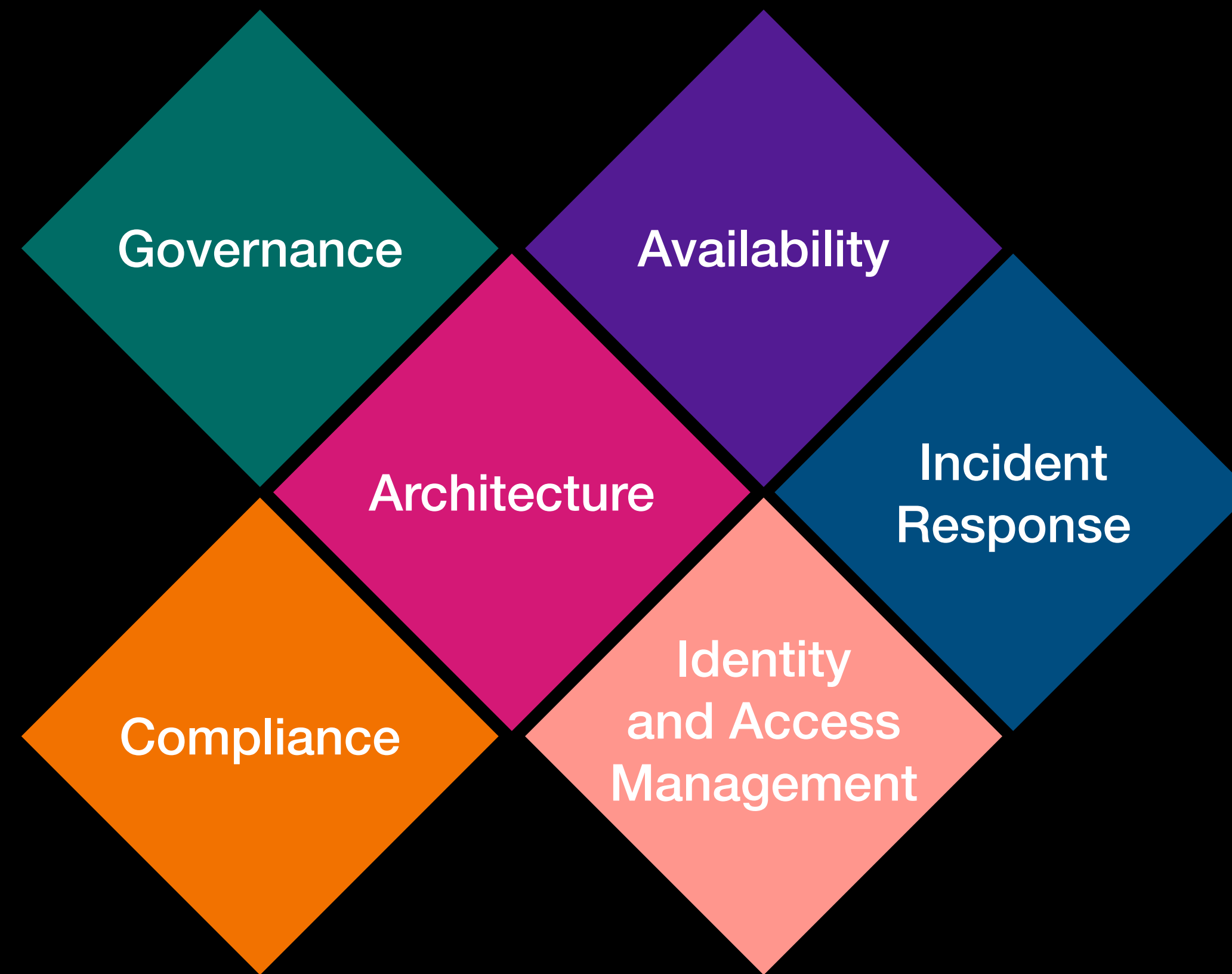


**Denial of
Service**

- Denial of Service attack involves overwhelming infrastructure so that it is not able to service legitimate requests.
- Denial of Service attacks can represent a significant threat to cloud providers and can result in unplanned downtime.

The Ugly

Cloud Computing



The Ugly

Cloud Computing



Identity
and Access
Management

The Ugly

Cloud Computing



Identity and Access Management

- Enterprises need to ensure only authorised individuals are able to access and process data.
- Challenge for enterprise is to ensure that access is managed effectively otherwise employees may be able to perform malicious actions.
- Poor management of identity and access could also lead to an increase in non-malicious actions.

The Ugly

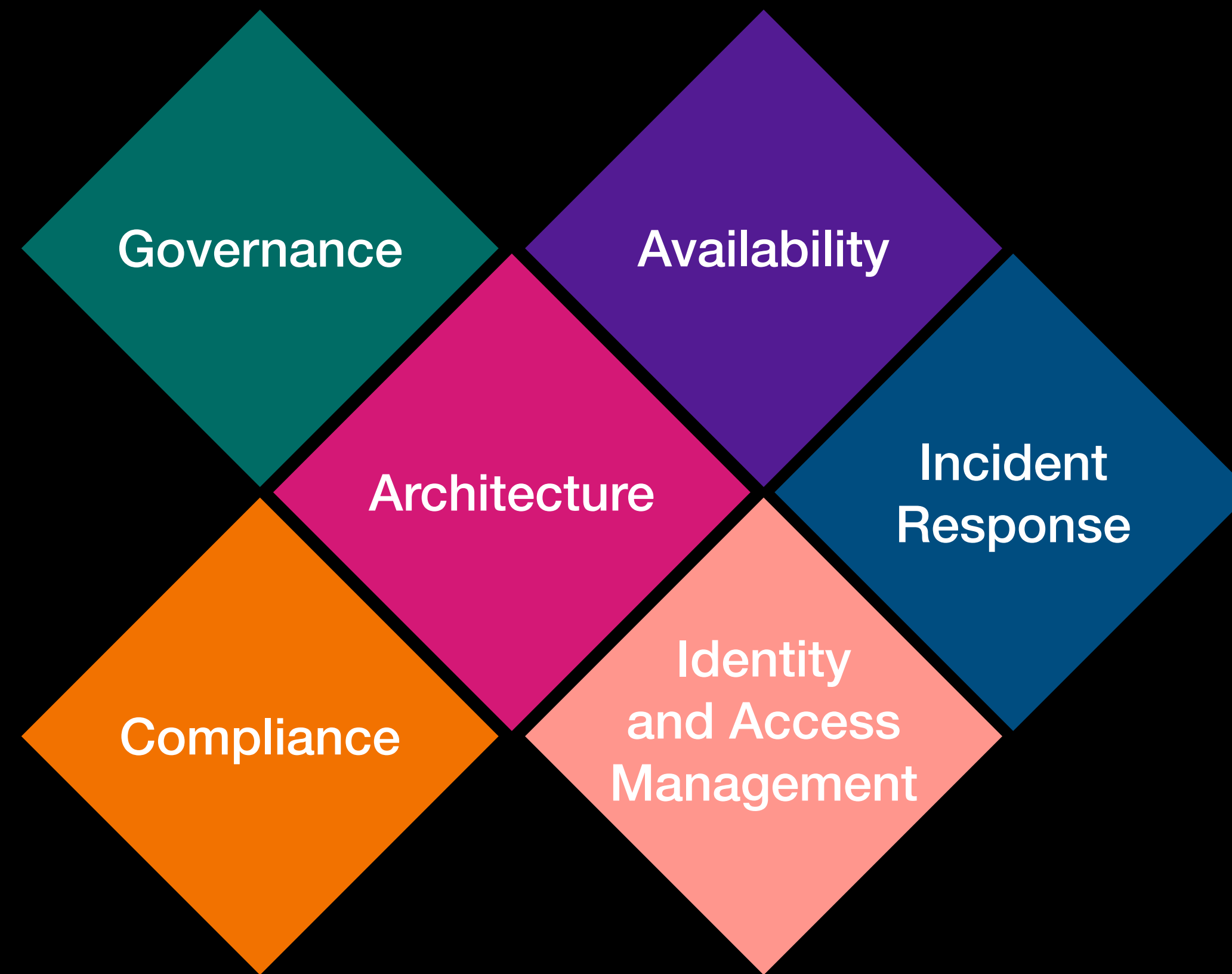
Cloud Computing



Identity
and Access
Management

The Ugly

Cloud Computing



The Ugly

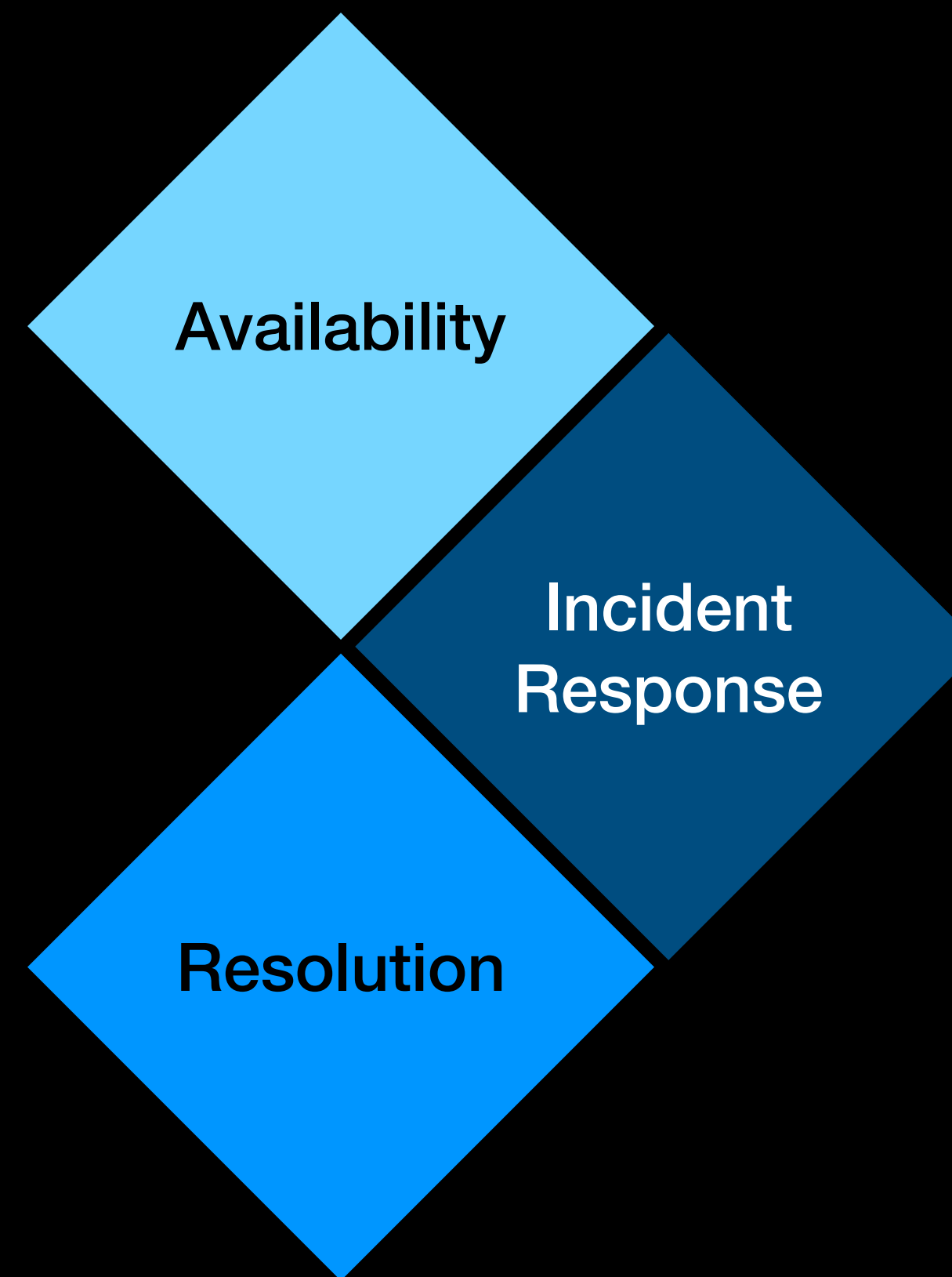
Cloud Computing



Incident
Response

The Ugly

Cloud Computing



The Ugly

Cloud Computing



Incident Response

- Cloud providers and enterprises need to process or an effective approach to respond in response of an attack.
- Complexity of cloud provider infrastructure can make it difficult to properly respond to incidents, especially if enterprises do not have a clear outlook on what data and services they have on cloud provider infrastructure or on-premises.

The Ugly

Cloud Computing



Availability

- Availability of data to support incident response is often poor for many cloud providers.
- Cloud providers may be reluctant to share data on vulnerabilities or provide sufficient access to detect events or issues with infrastructure (as it may promote enterprises to seek other cloud providers).
- Detail of data does depend on whether the offering is IaaS, PaaS or SaaS.

The Ugly

Cloud Computing

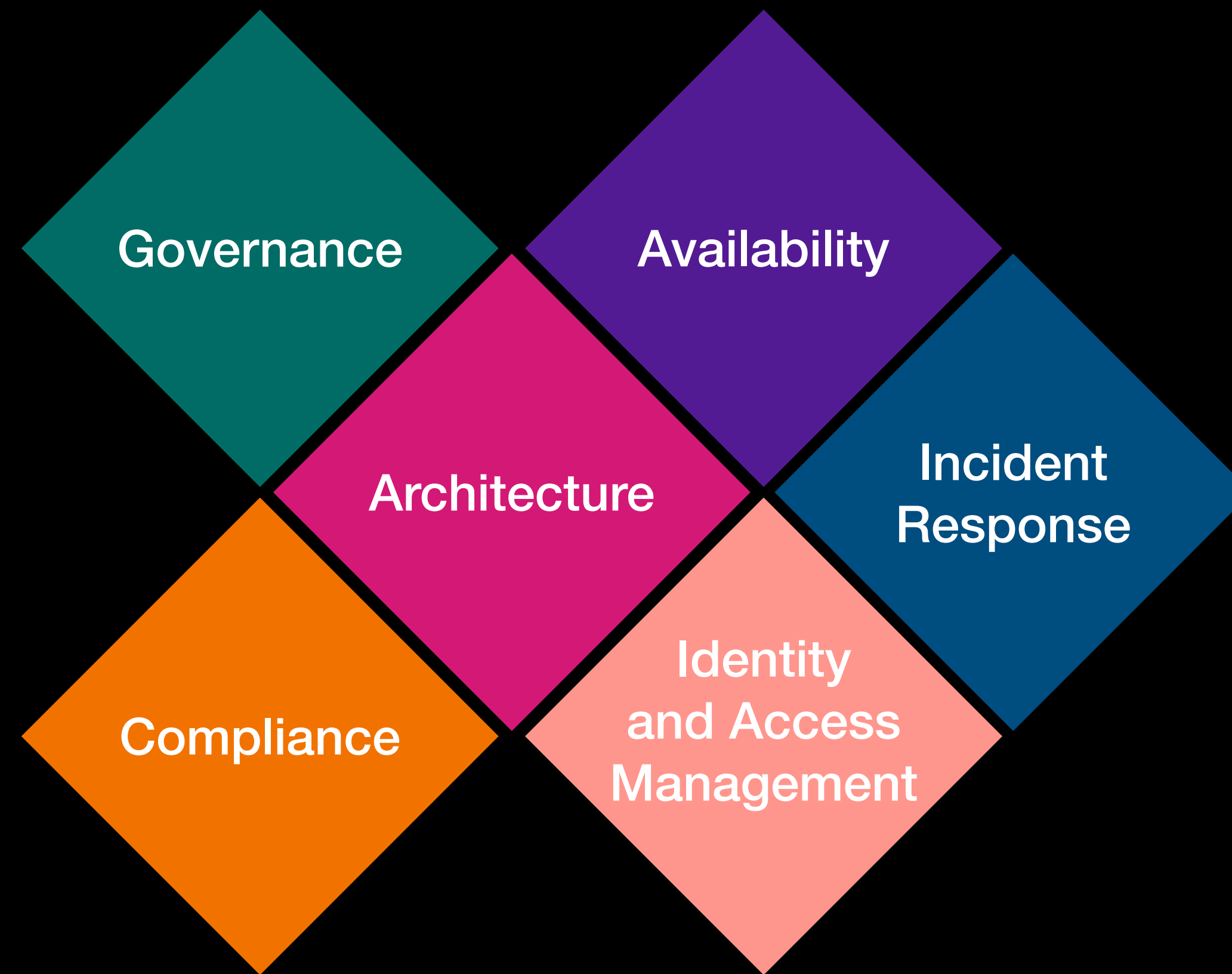


Resolution

- Response to an incident needs to be performed quickly, but data needs to be collected and the incident and response must be documented thoroughly.
- Incident response action as well as detail around the incident may become involved in legal proceedings and investigations.
- Resolution depends on the offering from the provider in terms of IaaS, PaaS or SaaS.

The Ugly

Cloud Computing



The Good,
the Bad
and the Ugly.

The Good,
the Bad
and the Ugly.

Security and Privacy of Cloud Computing

Architecture