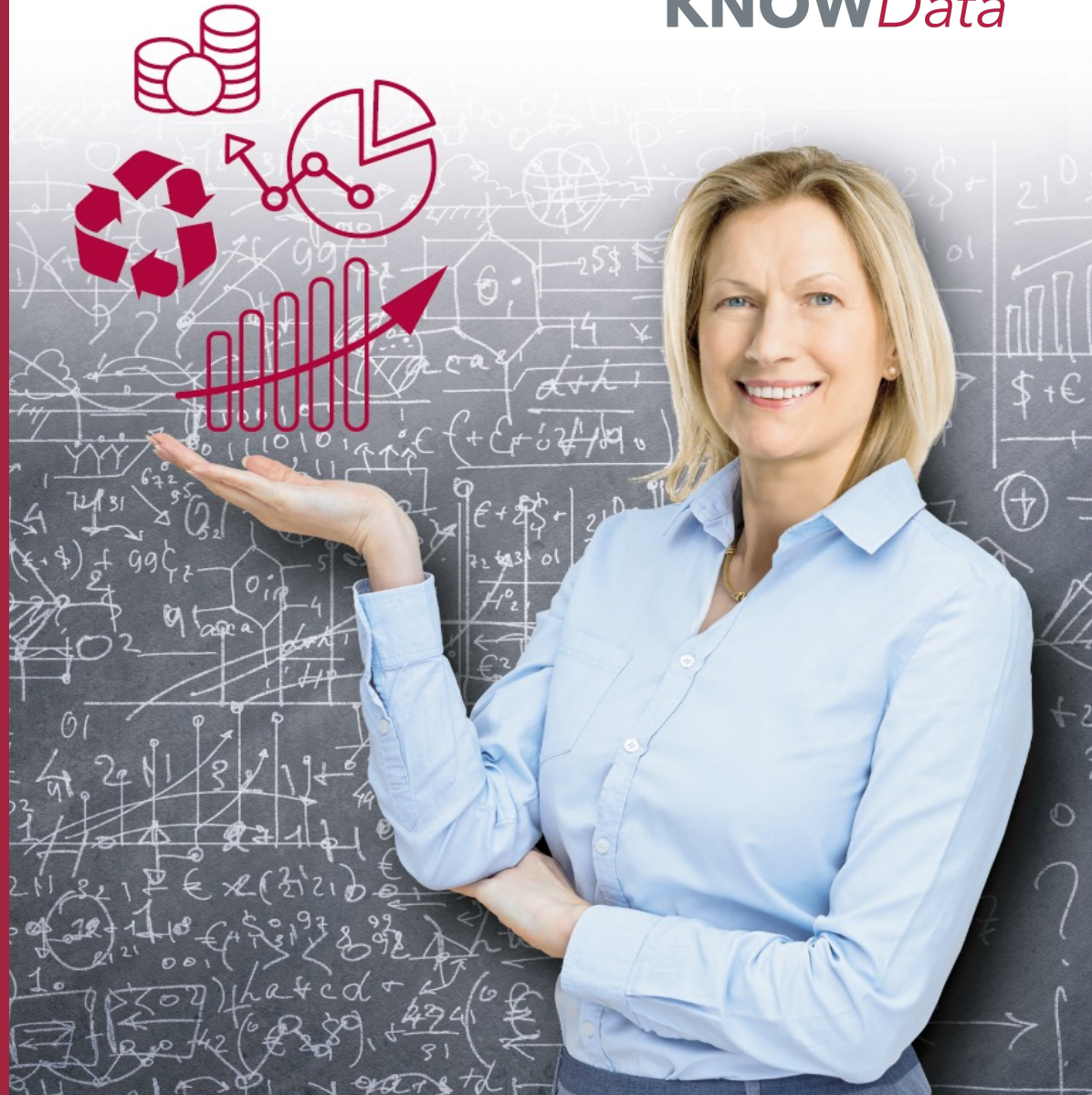


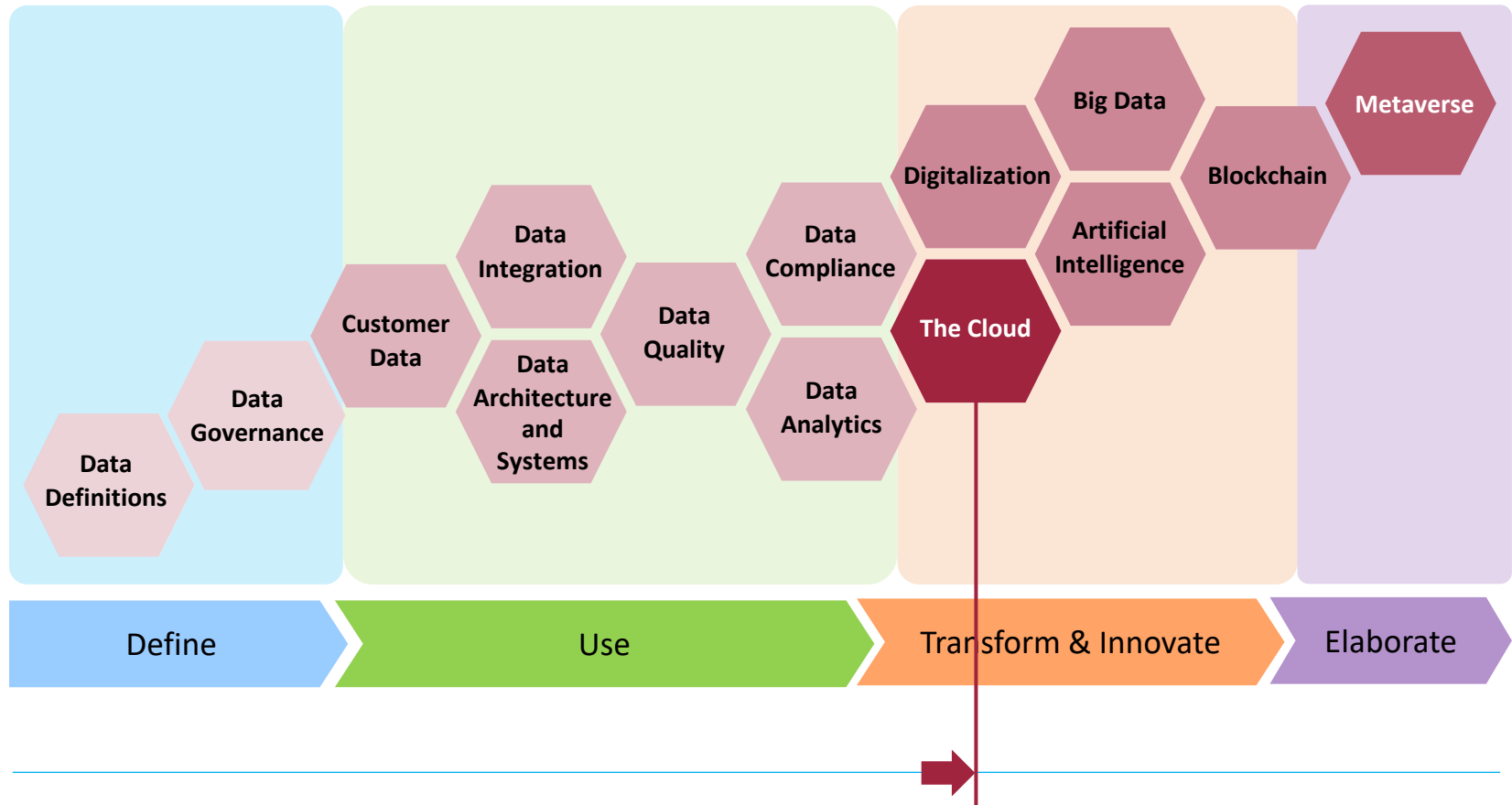
The Cloud



KNOW*Data*



October 12, 2026
Lionel Pilorget



Structure of the presentation



The Cloud

Cloud Services

IT as Self-service

XaaS

Cloud-native
principles

Cloud Usage

Cloud Data Protection Framework

Personal Data

Regulations



Location

Operation &
Processes

Journey to the Cloud

Cloud Migration



Management of
Cloud Services

Hybrid Multi-
Cloud
Architecture

Cloud
Transformation

Cloud Computing of the Future

Distributed
Cloud

Serverless
Computing

Service Mesh

Neurodata



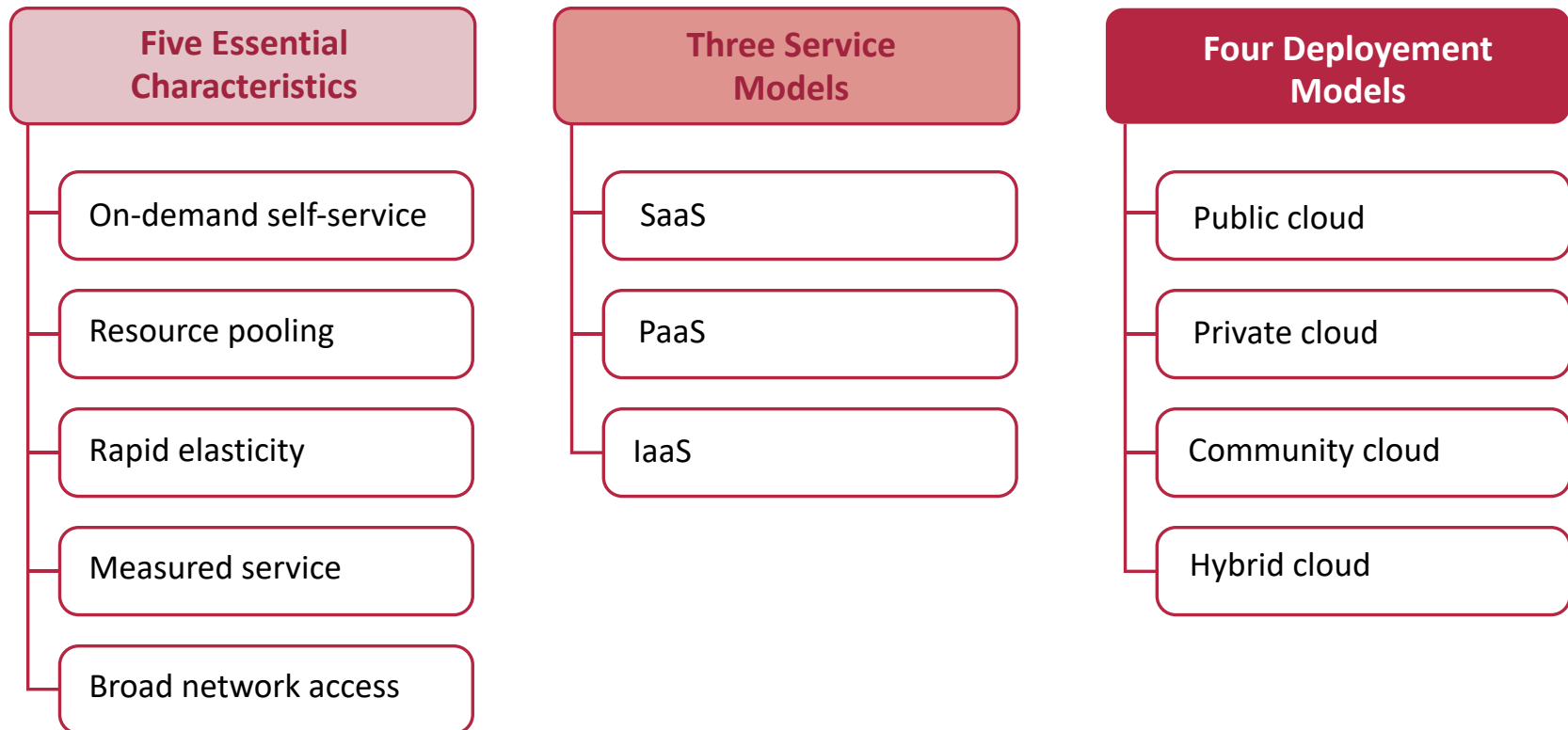
IT as self-service

Definition of Cloud Computing



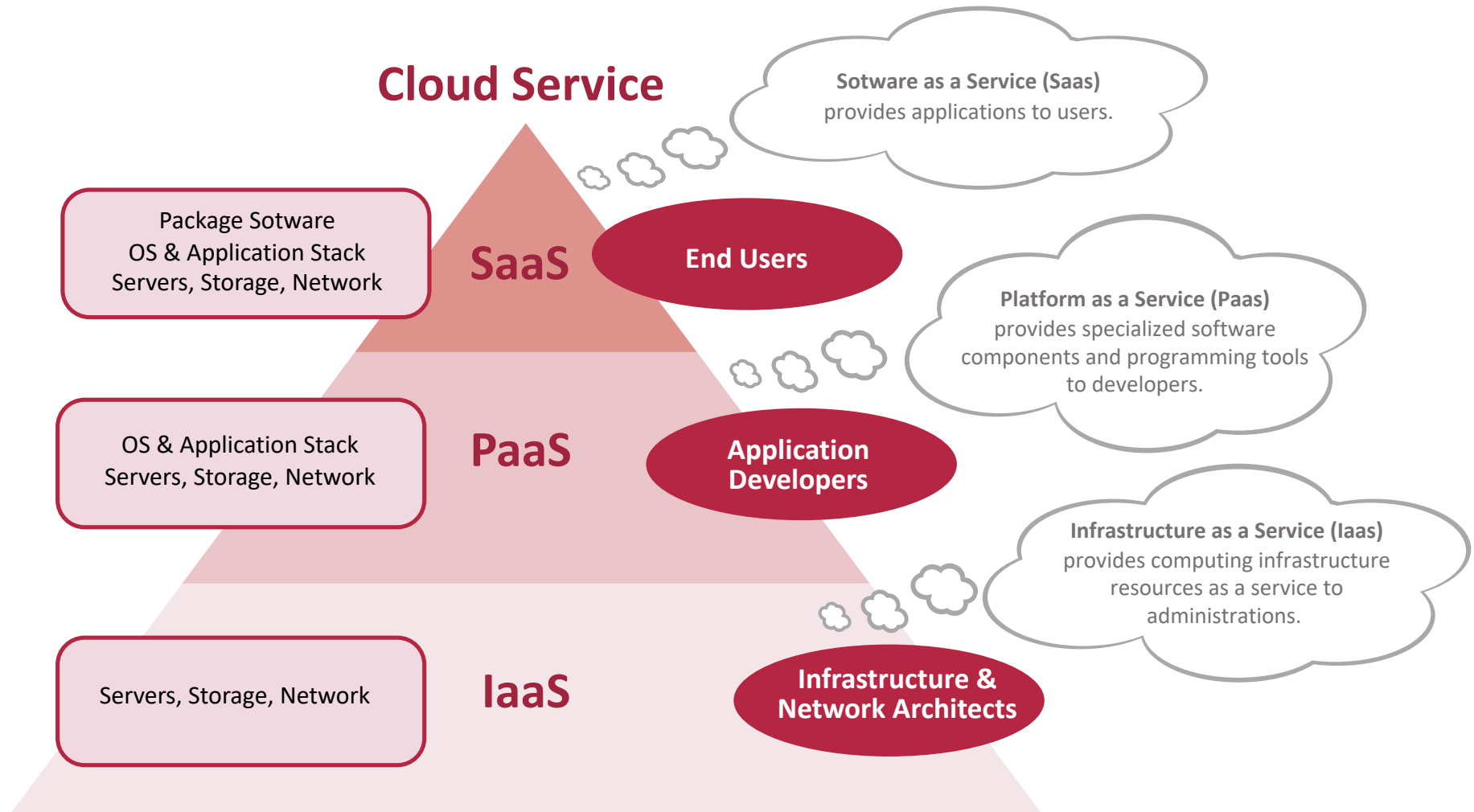
Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

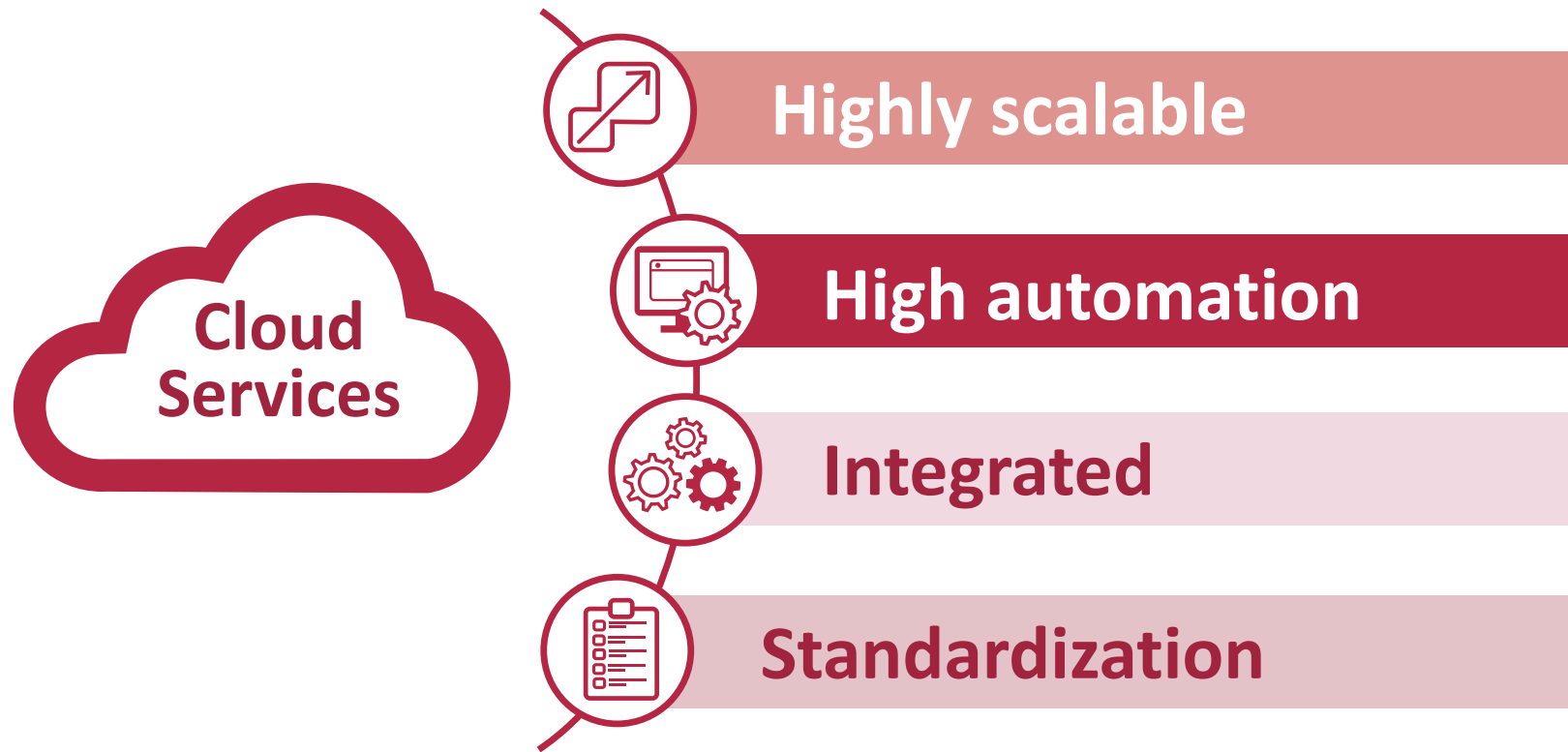
Definition according to NIST (2011): <https://csrc.nist.gov/publications/detail/sp/800-145/final>





Cloud Service

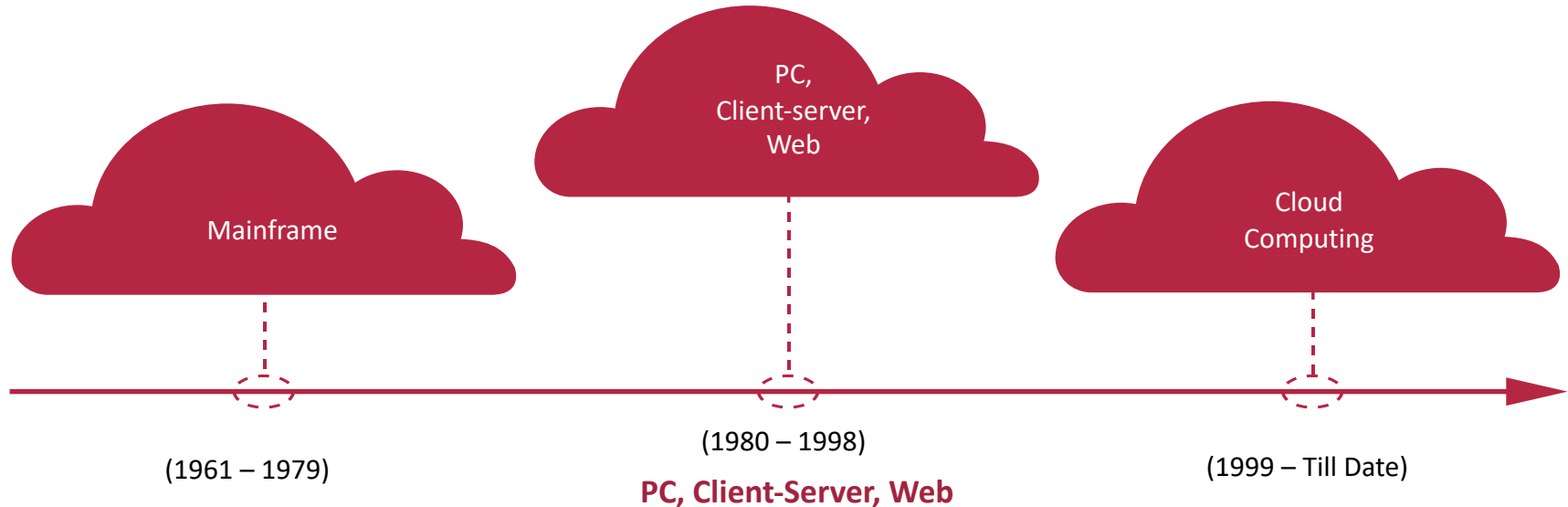




➔ Multi-tenancy + Measured service (pay-per-use) + API-driven infrastructure
These features increase flexibility but reduce visibility and control.



centralization → decentralization → hyperscaler



- 1980 – Popularity onf the PC, client-server model
- 1961 – The World Wide Web (WWW) popularizes the internet
- 1997 – First use of the term “Cloud Computing”

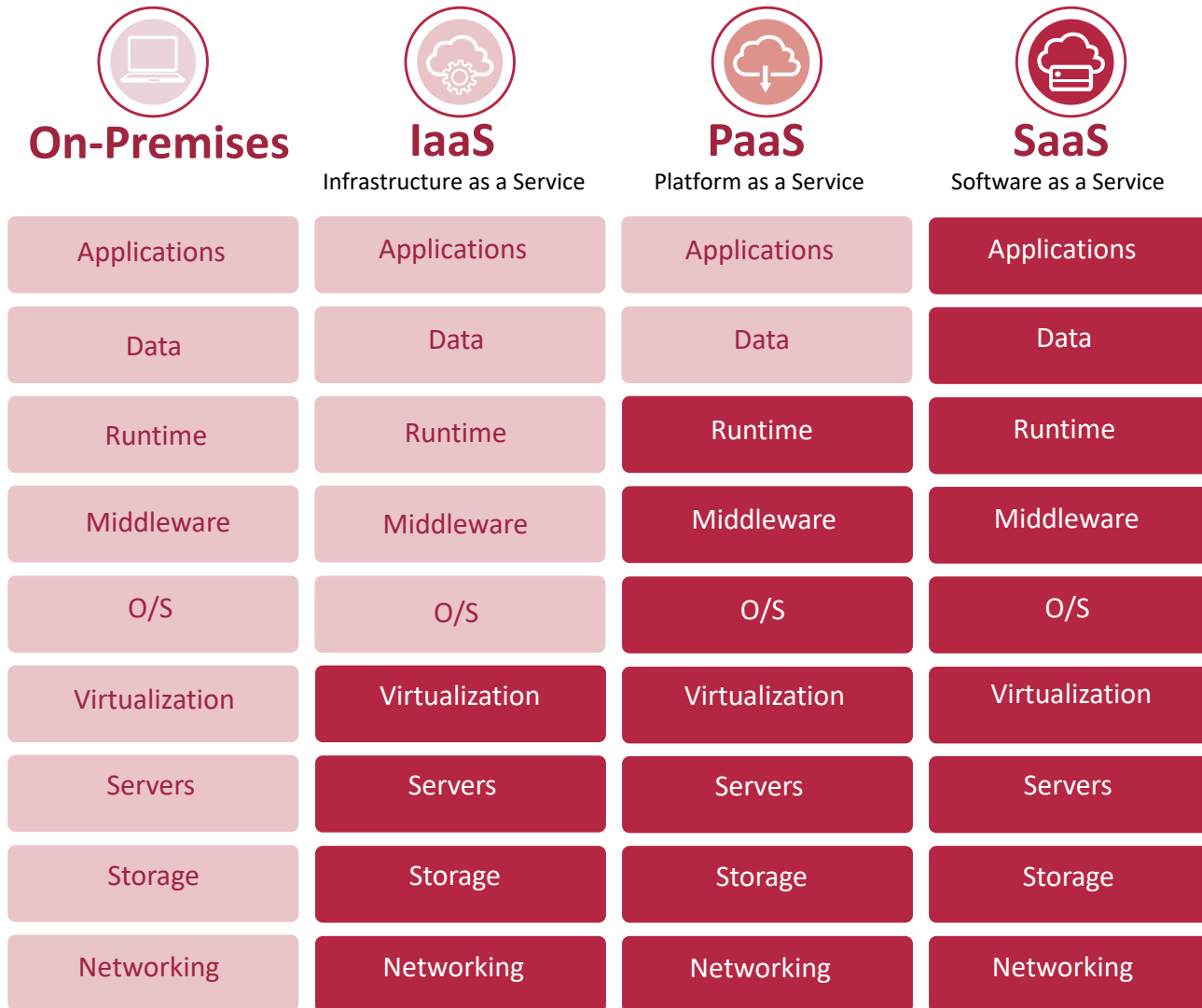
Mainframe

- 1961 – Professor John McCarthy proposes computing as „ public utility“
- 1964 – IBM CP-40 opeating systems uses virtualization
- 1972 – IBM VM/370 is a virtual machine operating system

Cloud Computing

- 1999 – Salesforce.com and VMWare launch
- 2002 – Amazon Web Services (AWS) launches and SOA emerges
- 2006 – Hadoop launched, shortly followed by amazon S3 and Amazon EC2
- 2007 – Salesforce introduces Force.com
- 2008 – Google App Engine launches
- 2009 – Microsoft Azure launches

Shared Responsibility Model



O/S: Operating System



You Manage



Other Manages



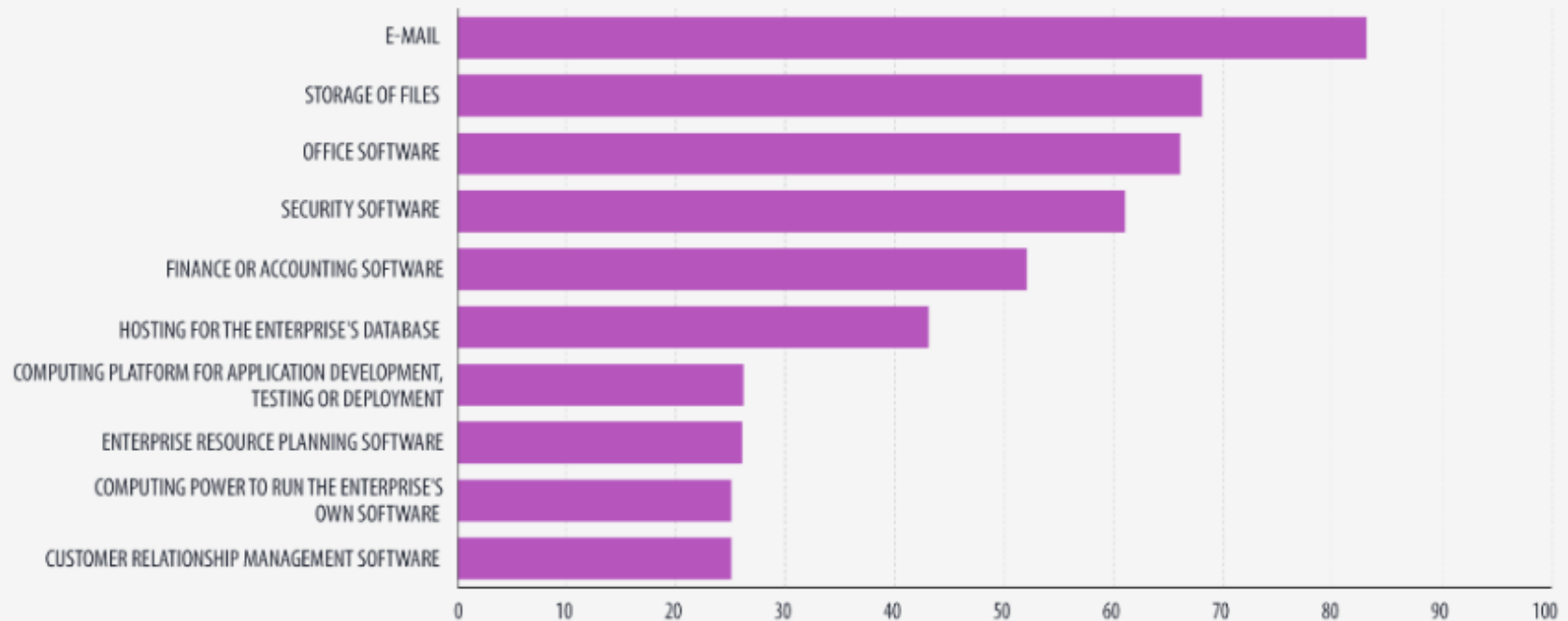
Also relevant for on-premise infrastructure

- **Microservices:** Design applications as loosely coupled, independent services, allowing for separate development, deployment, and scaling.
- **Containerization:** Package applications and their dependencies into portable containers for consistent environments.
- **Orchestration:** Use tools (like Kubernetes) to automate container deployment, scaling, and management.
- **Automation (DevOps/CI/CD):** Automate the entire lifecycle (build, test, deploy, repair, scale) for speed and consistency.
- **Resilience:** Build for failure with redundancy, self-healing, and disaster recovery to remain available.
- **Scalability & Elasticity:** Design for horizontal scaling (adding more instances) to handle varying loads efficiently.
- **Observability:** Implement deep monitoring and logging to understand system behavior and diagnose issues quickly.
- **Statelessness** (where possible): Design components to not store session data, making them easier to scale and replace.
- **Immutable Infrastructure:** Treat servers as disposable; replace them rather than updating them in place



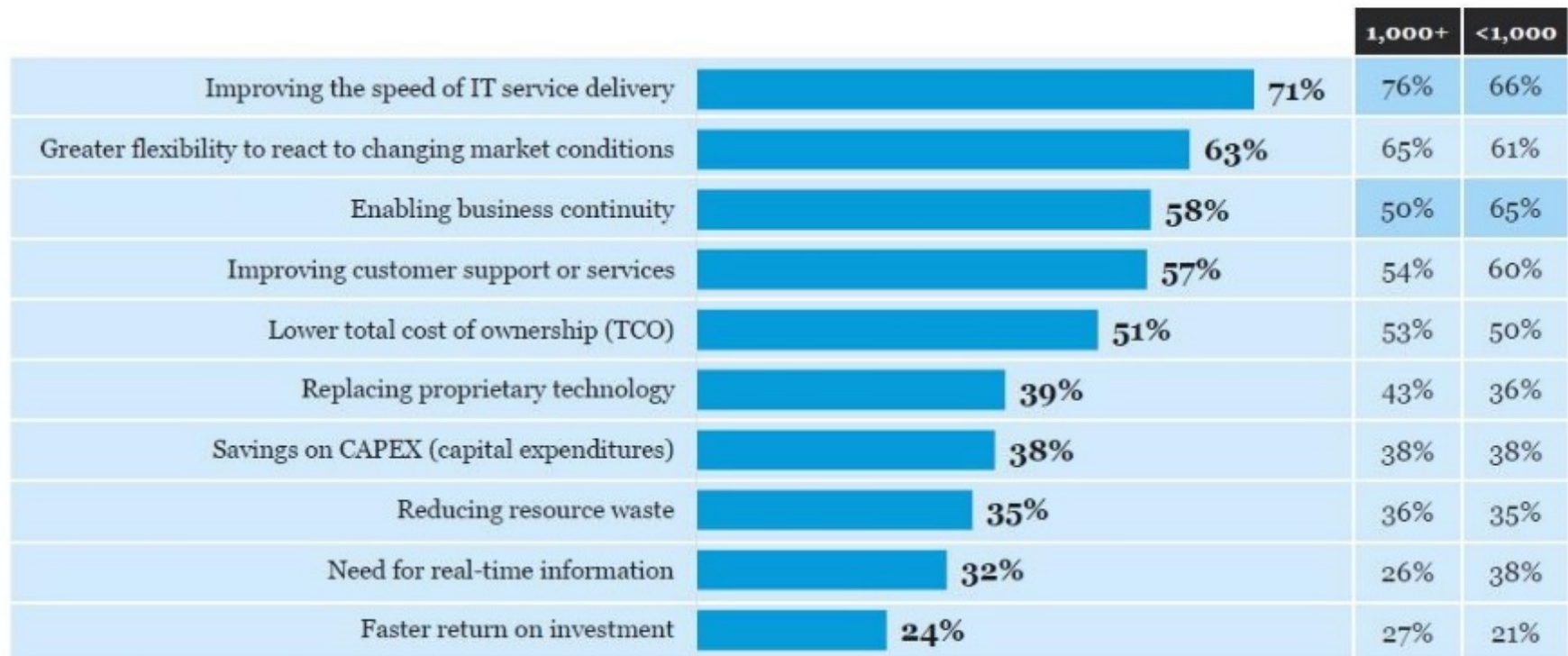
Cloud computing services purchased by EU enterprises in 2023

(% of enterprises that purchased a cloud computing service)





Cloud Solutions Are Feeding the Need for Speed



Q. Please rank the top business goals or objectives that are driving investments in cloud computing initiatives at your organization.



1. **Accessibility:** With cloud storage, data is accessible from anywhere, anytime, and on any device, giving employees more flexibility to work remotely.
2. **Collaboration:** Cloud storage allows team members to easily share and collaborate on files.
3. **Scalability:** Cloud storage enables organizations to scale their storage capacity as their data grows, eliminating the need for constant hardware upgrades.
4. **Disaster recovery:** Cloud storage providers typically have a disaster recovery plan in place. However, organizations must ensure that they have a comprehensive backup and recovery strategy to protect their data even in the event of a cloud outage or data loss.
5. **Cost:** Cloud storage can reduce costs associated with physical hardware, such as purchasing and maintaining servers.
6. **Security:** cloud providers offer robust security with encryption & redundancy (data mirrored across locations), only if configured correctly.
7. **Automated Updates:** cloud providers handle software updates & maintenance, reducing the burden on internal IT teams.
8. **Data Synchronization:** keep files consistency across all devices automatically.

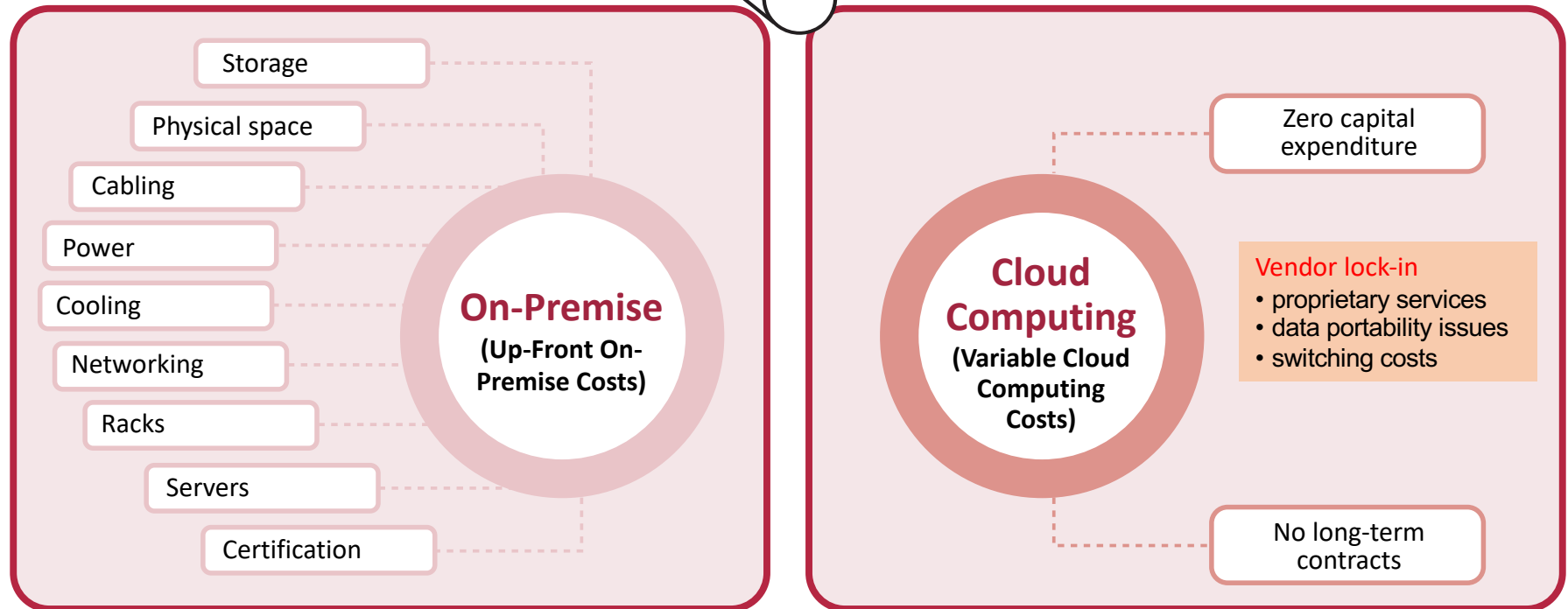
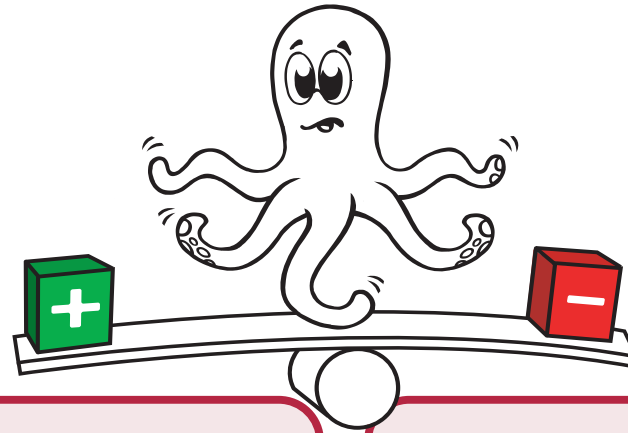


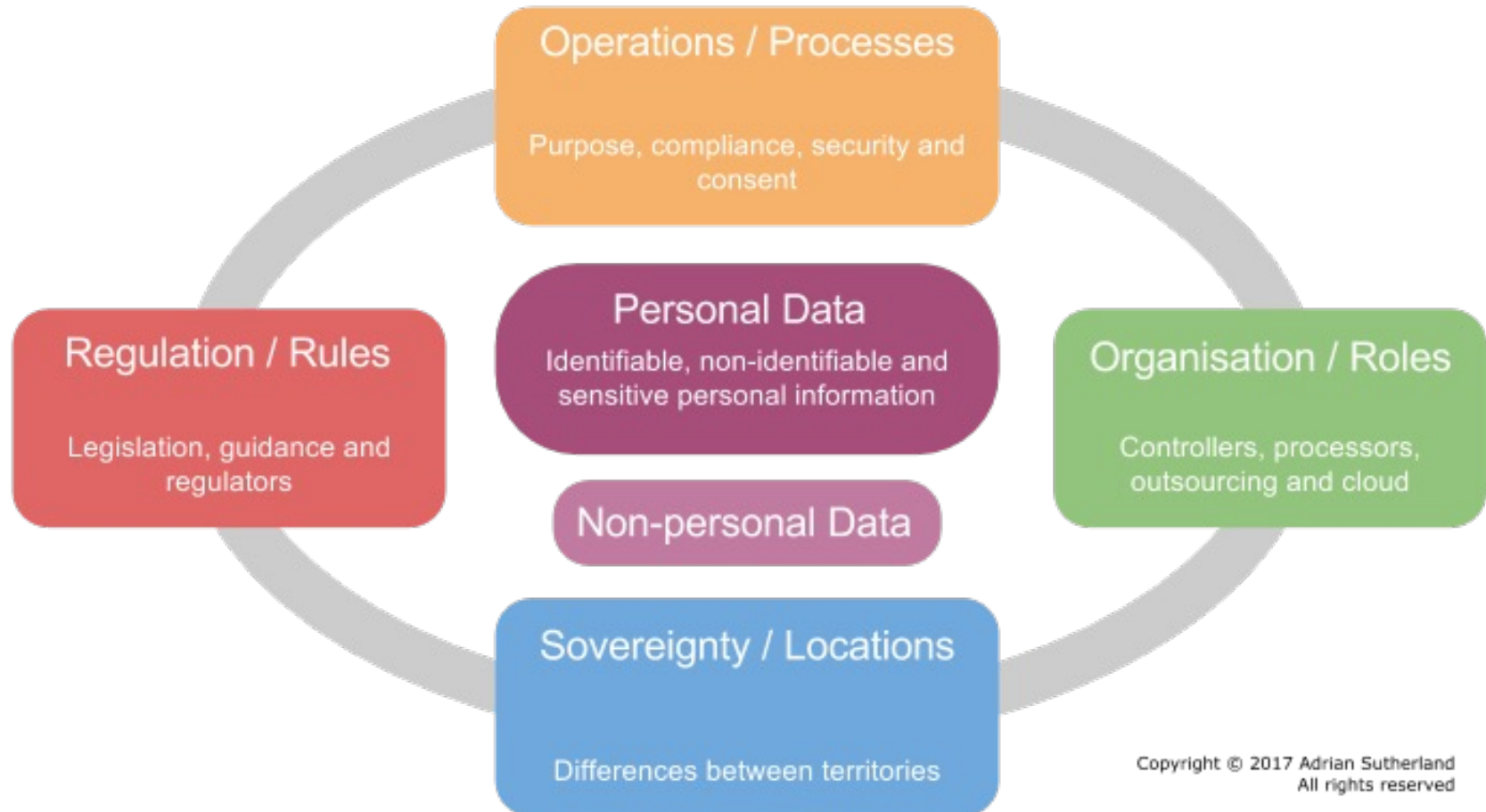
Of course, risks should be taken into account !
Like data leakage risk, cost unpredictability, misconfiguration risk...

Question: On-Premise versus Cloud Computing?



Advantages and disadvantages of both solutions

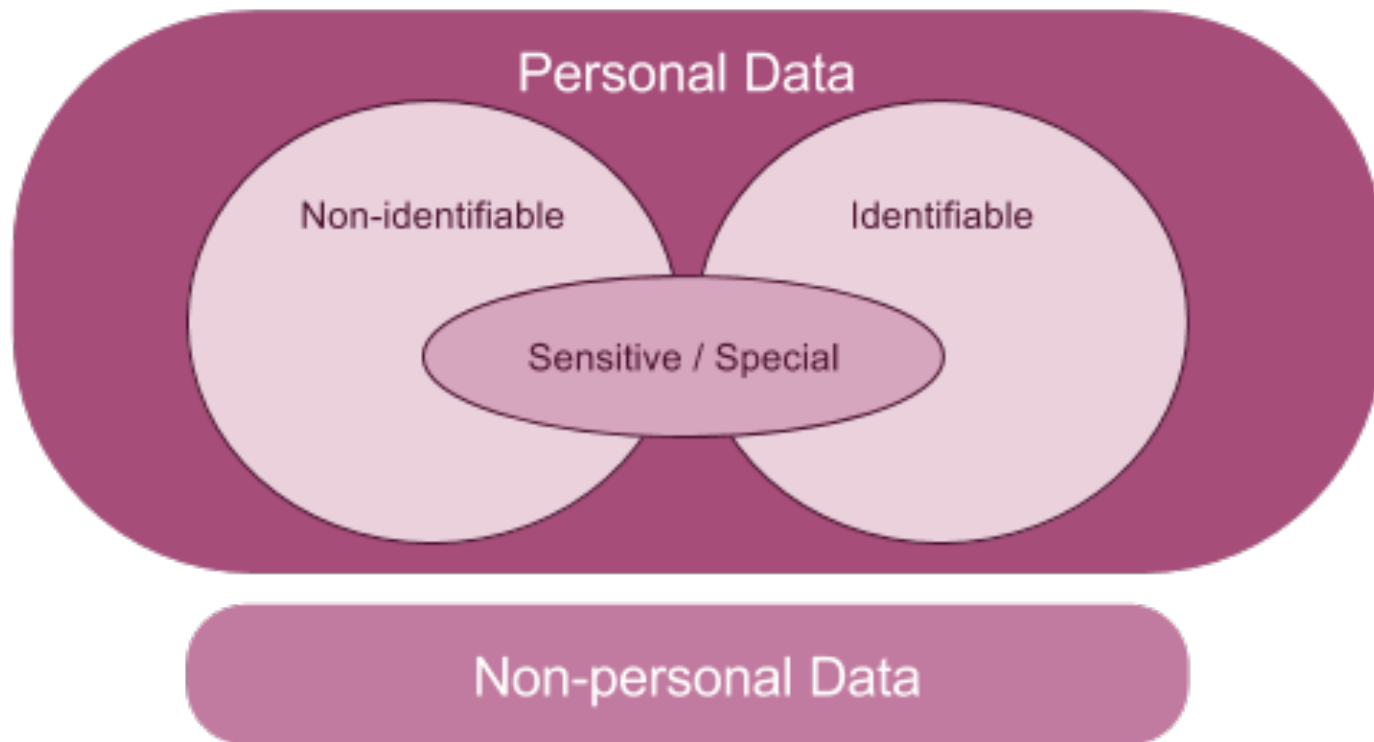




The Importance of Data



Data classification drives governance decisions





Information that does not identify an individual, either directly or indirectly



Technical & Machine Data

- Server CPU usage
- Network latency measurements
- Error rates in an application
- System uptime percentages
- Software version usage statistics



- IP addresses



Environmental & Geographic Data

- Average monthly rainfall in a region
- Air quality index (AQI)
- Soil moisture levels
- River water levels
- Elevation or terrain maps



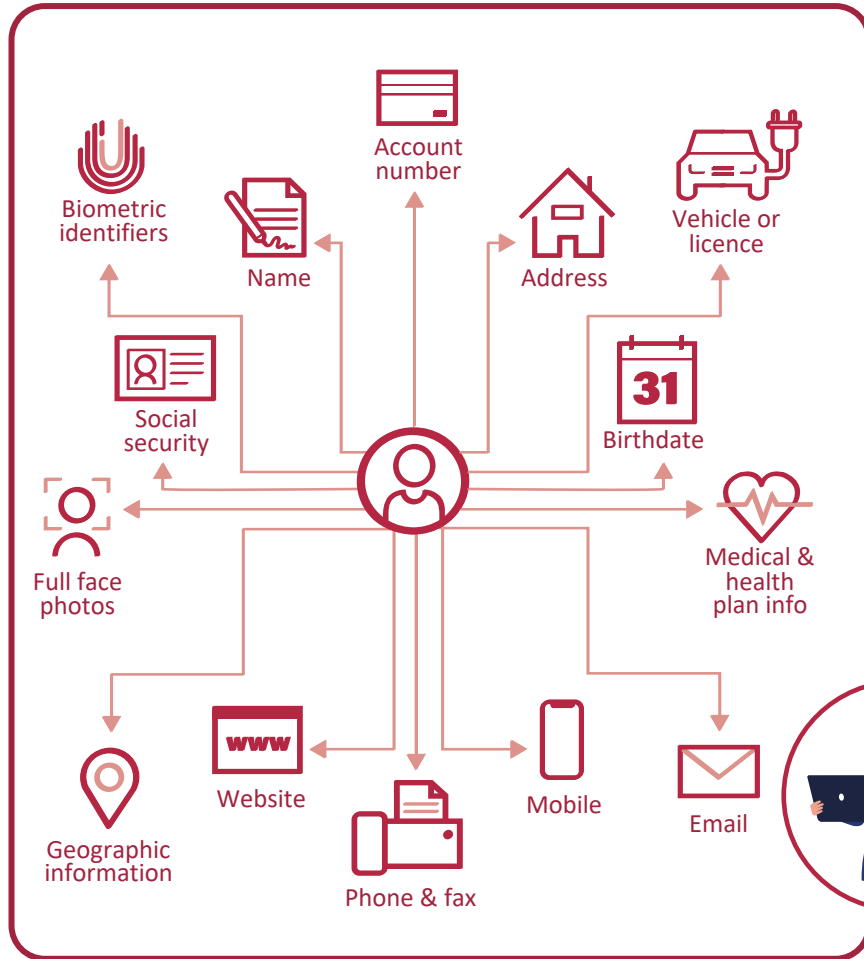
Business & Economic Data

- Company's annual revenue
- Number of products sold per quarter
- Market share by industry
- Inventory stock levels
- Average delivery time

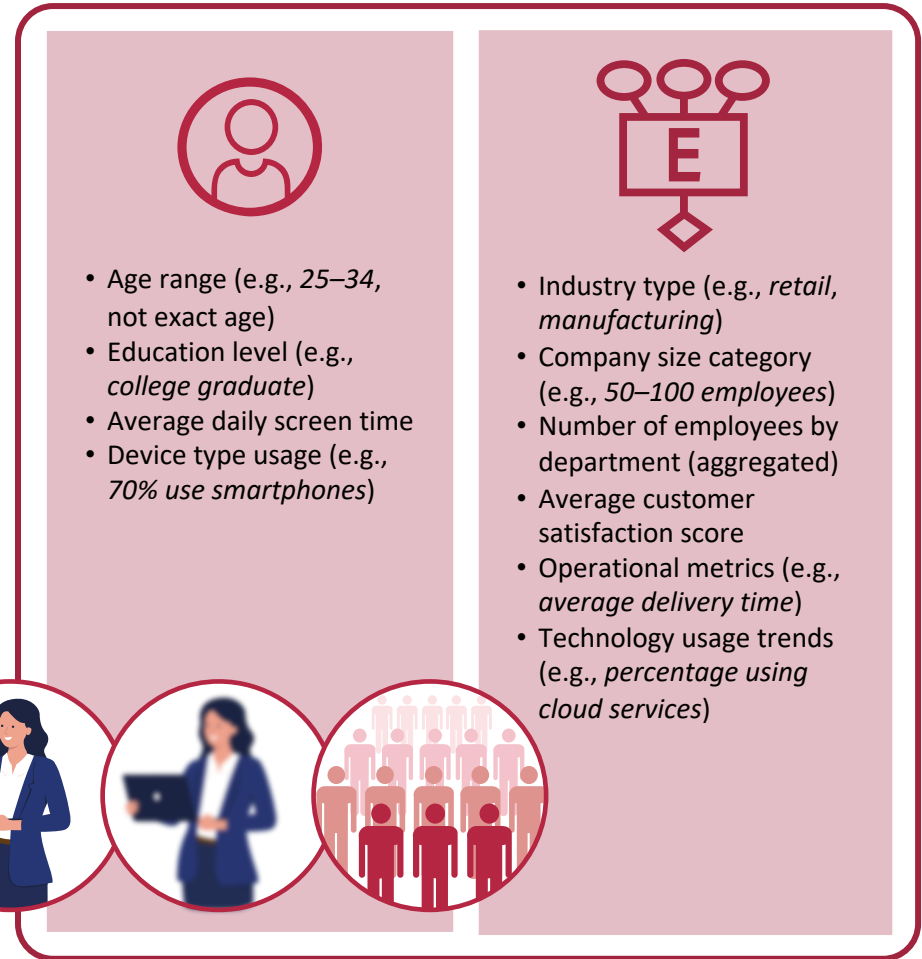
Identifiable and Non-Identifiable Data



Identifiable: identify, contact, or locate a single person



Non-Identifiable: de-identified, or that could not lead to personally identifiable information

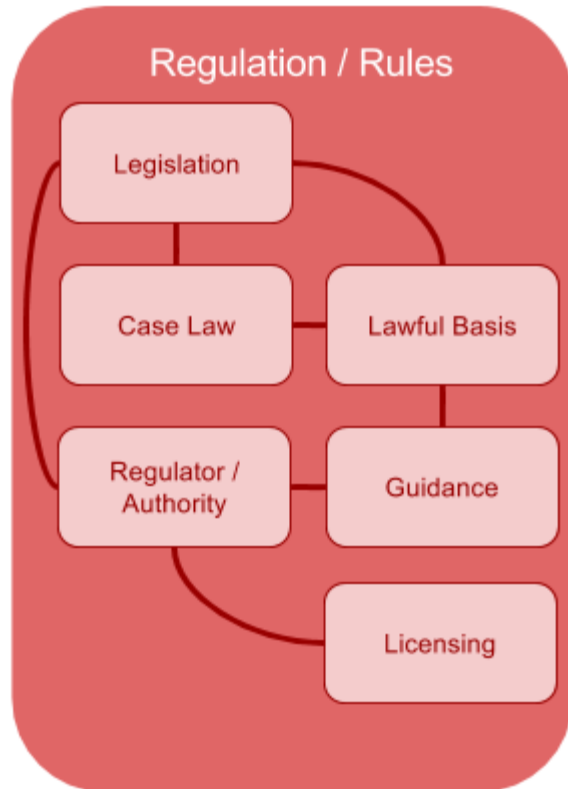




If you move sensitive data to the cloud, you are not just making a technical decision—you are making a high-stakes governance and compliance decision

The following personal data is considered **‘sensitive’** and is subject to specific processing conditions:

- personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs;
- trade-union membership;
- genetic data, biometric data processed solely to identify a human being;
- health-related data;
- data concerning a person’s sex life or sexual orientation.



Examples

- General Data Protection Regulation (EU)
- Federal Act on Data Protection (Switzerland)
- Personal Information Protection and Electronic Documents Act (Canada)
- Digital Personal Data Protection Act, 2023 (India)
- Personal Information Protection Law (China)
- Lei Geral de Proteção de Dados Pessoais - General Personal Data Protection Law (Brazil)



What happens if this fails?

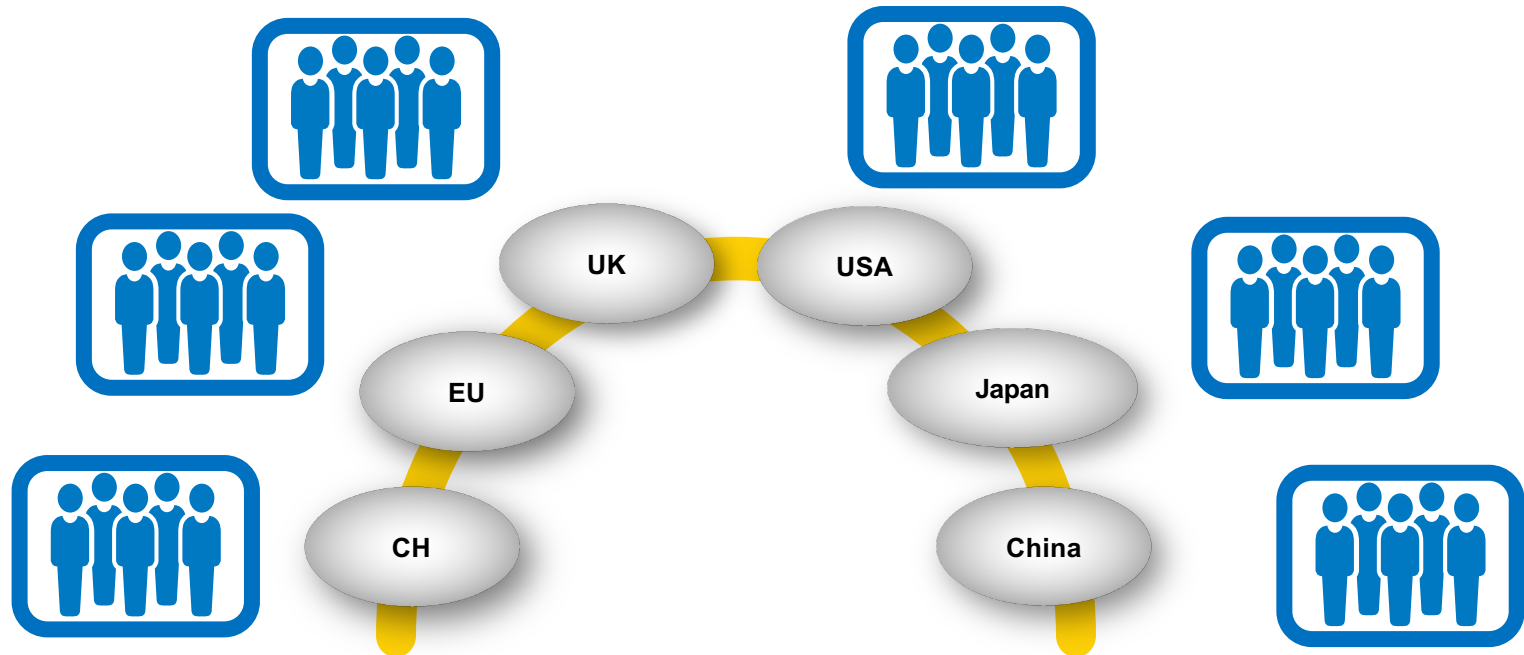
Subject	Cloud Provider	Cloud Customer
Governance & Accountability	- Clearly define role (Processor / Sub-processor) - Publish privacy notice and data processing terms - Maintain records of processing activities - Assign a Data Protection Officer (DPO) - Support customer compliance obligations	- Define role (Controller / Data Fiduciary) - Document lawful basis for processing - Maintain internal data inventory - Appoint DPO / privacy contact if required - Conduct vendor risk assessments
Contracts & Legal Agreements	- Offer compliant Data Processing Agreement (DPA) - Specify sub-processors and update mechanisms - Include audit rights or third-party certifications - Define breach notification timelines - Support cross-border transfer clauses (e.g., SCCs)	- Execute DPA before processing data - Review sub-processor list and object if needed - Ensure transfer mechanisms are valid - Align contract terms with regulatory obligations - Retain right to terminate for non-compliance
Data Security	- Encryption in transit and at rest - Strong access controls and IAM - Logging and monitoring - Regular vulnerability scanning and patching - Physical security of data centres - Independent security certifications (ISO 27001, ...)	- Configure security controls correctly - Apply least-privilege access - Secure credentials and API keys - Enable logging and monitoring - Conduct regular security reviews
Data Location & Cross-Border Transfers	- Disclose data centre locations - Offer region-specific data residency options - Support transfer safeguards (SCCs, adequacy) - Enable localization where legally required (e.g., China)	- Select compliant regions - Assess international transfer risks - Obtain required approvals or assessments - Inform users about cross-border processing - Monitor regulatory changes
Data Subject / User Rights	- Provide tools for data access, deletion, export - Support portability formats - Enable secure data erasure	- Handle user rights requests - Verify user identity - Coordinate with provider for fulfilment - Respond within legal timelines
Breach Detection & Incident Response	- Maintain incident response plan - Detect and investigate breaches - Notify customers without undue delay - Provide incident details and remediation support	- Maintain breach response procedures - Notify regulators and users where required - Assess risk of harm - Document incidents and lessons learned

Which data protection laws for which country?



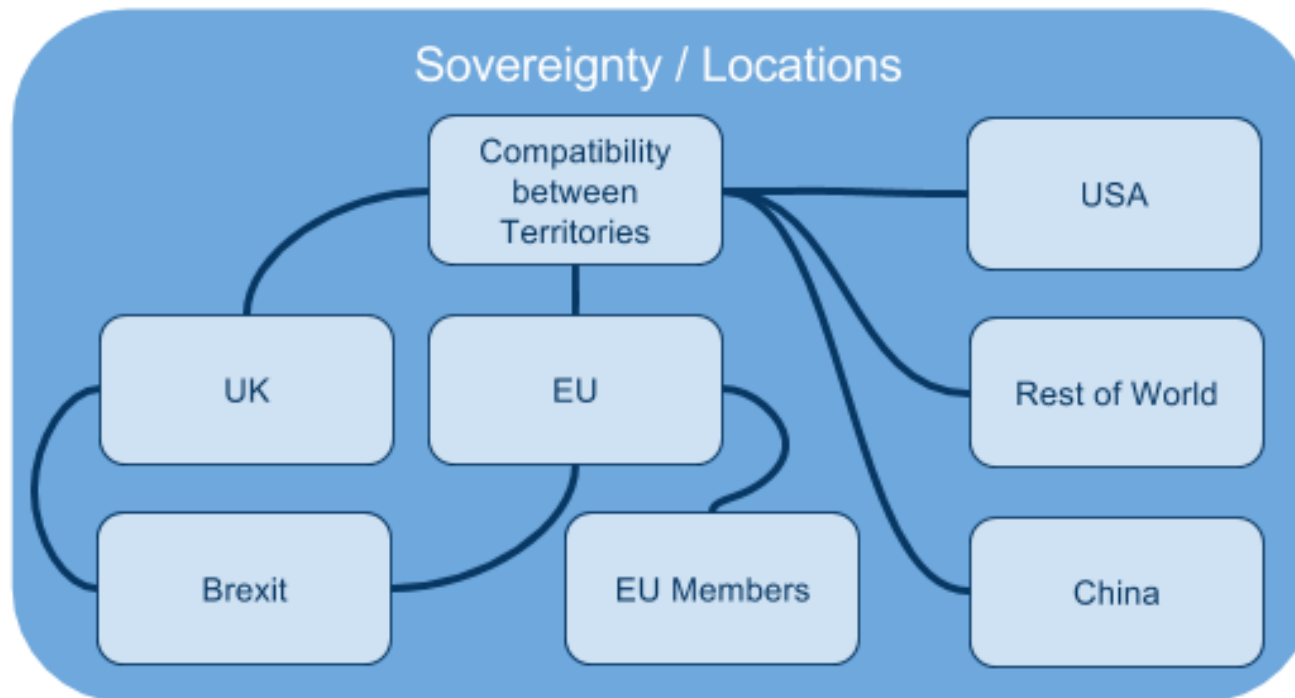
Please find the main guidelines concerning data protection applying to cloud solutions published by Data Protection Authorities (“DPA”)

- | | |
|-------------------|----------|
| 1. Switzerland | 4. USA |
| 2. European Union | 5. Japan |
| 3. UK | 6. China |



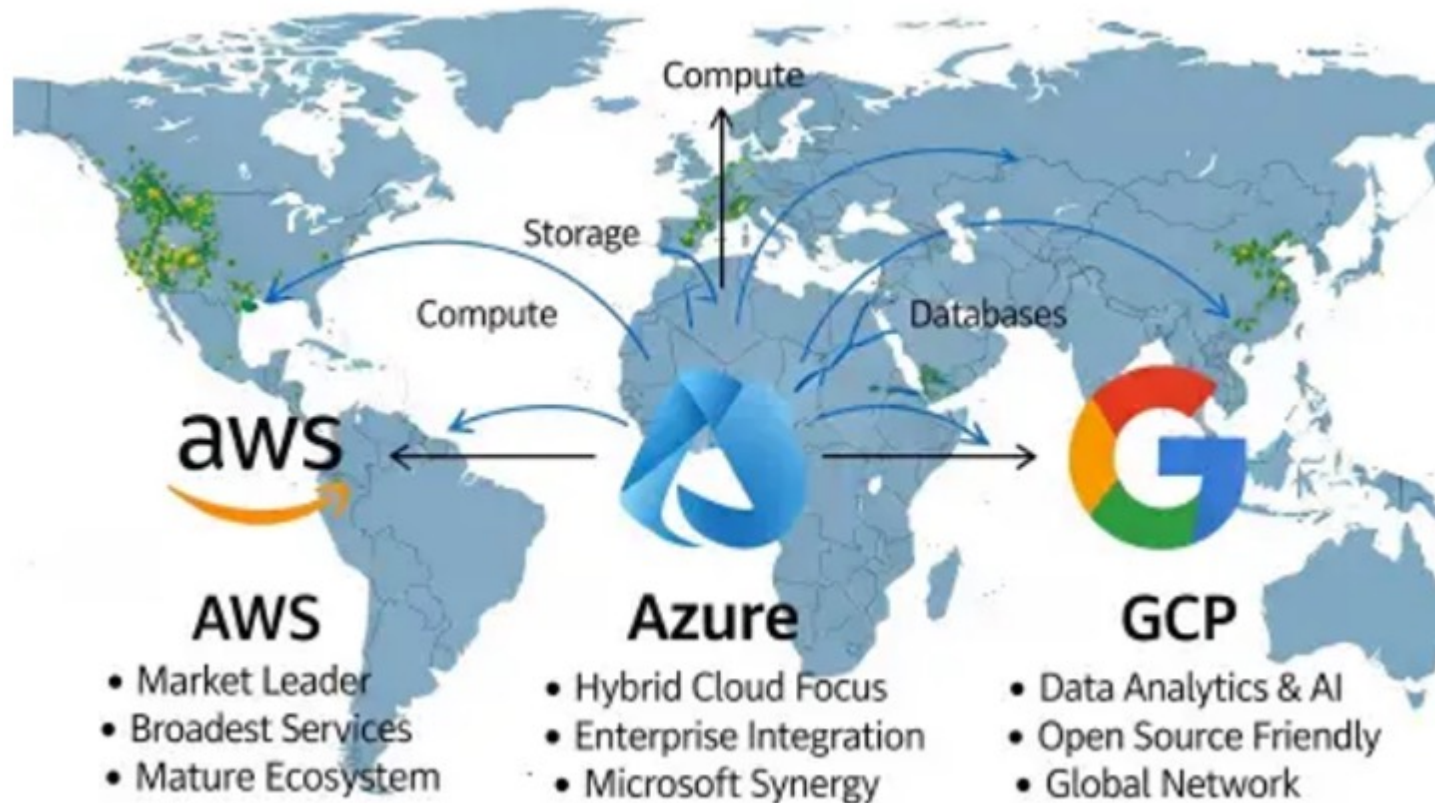


Data location determines applicable laws, breach notification obligations, and government access rights





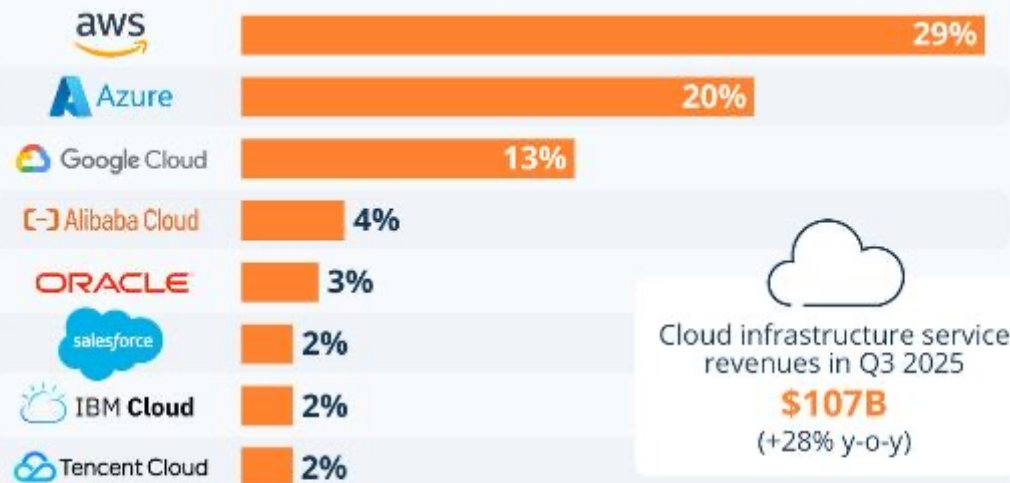
Geopolitical actors, not just providers





AWS Stays Ahead as Cloud Market Accelerates

Worldwide market share of leading cloud infrastructure service providers in Q3 2025*



* Includes platform as a service (PaaS) and infrastructure as a service (IaaS) as well as hosted private cloud services

Source: Synergy Research Group



statista

Who Uses What...



AWS



Azure



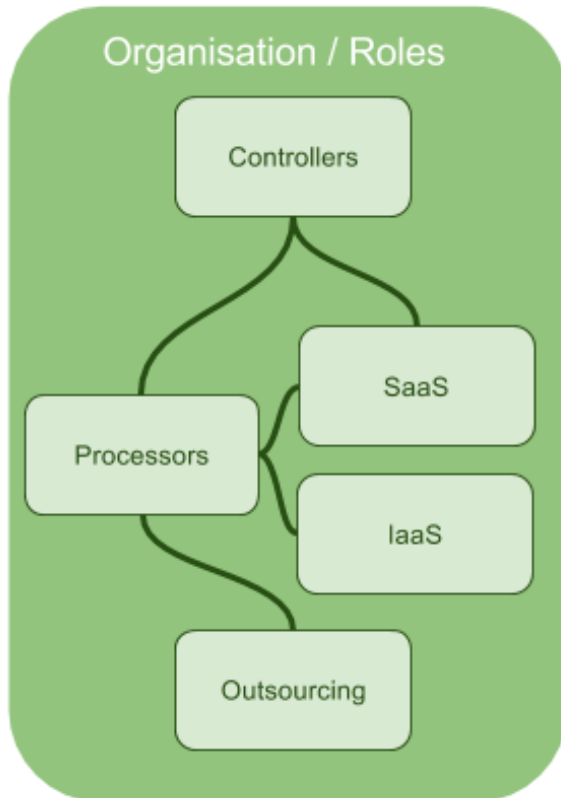
Google Cloud



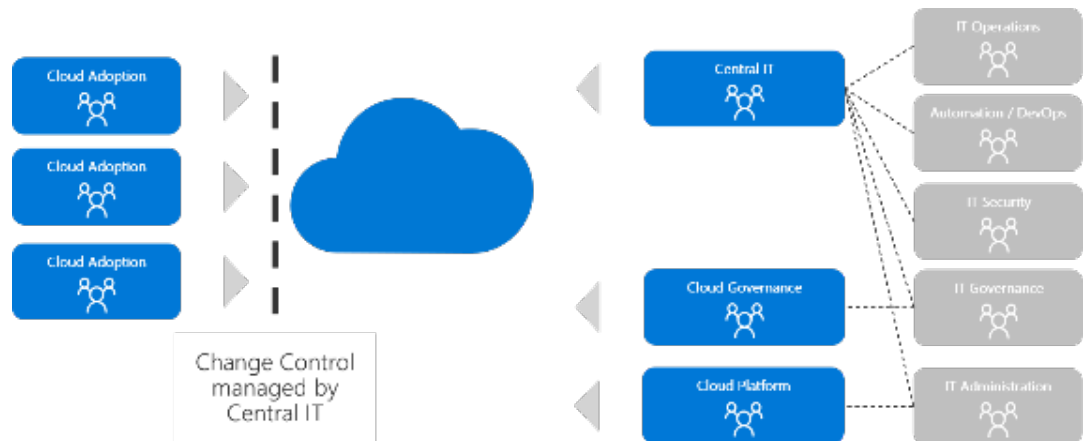
Who ultimately controls the data?

Since 2001, US companies have had to transmit all data collected to the US authorities. This is ensured by the **Patriot Act**, which, however, only applies to servers in the USA. In 2018, the US crossed all borders: since then, data stored abroad must also be passed on. The CLOUD Act ("Clarifying Lawful Overseas Use of Data Act") states that **it does not matter whether data is stored in the USA or outside**. As long as the company is based in the USA, the respective company must pass on all customer data upon request - or provide the authorities and intelligence services with a backdoor.





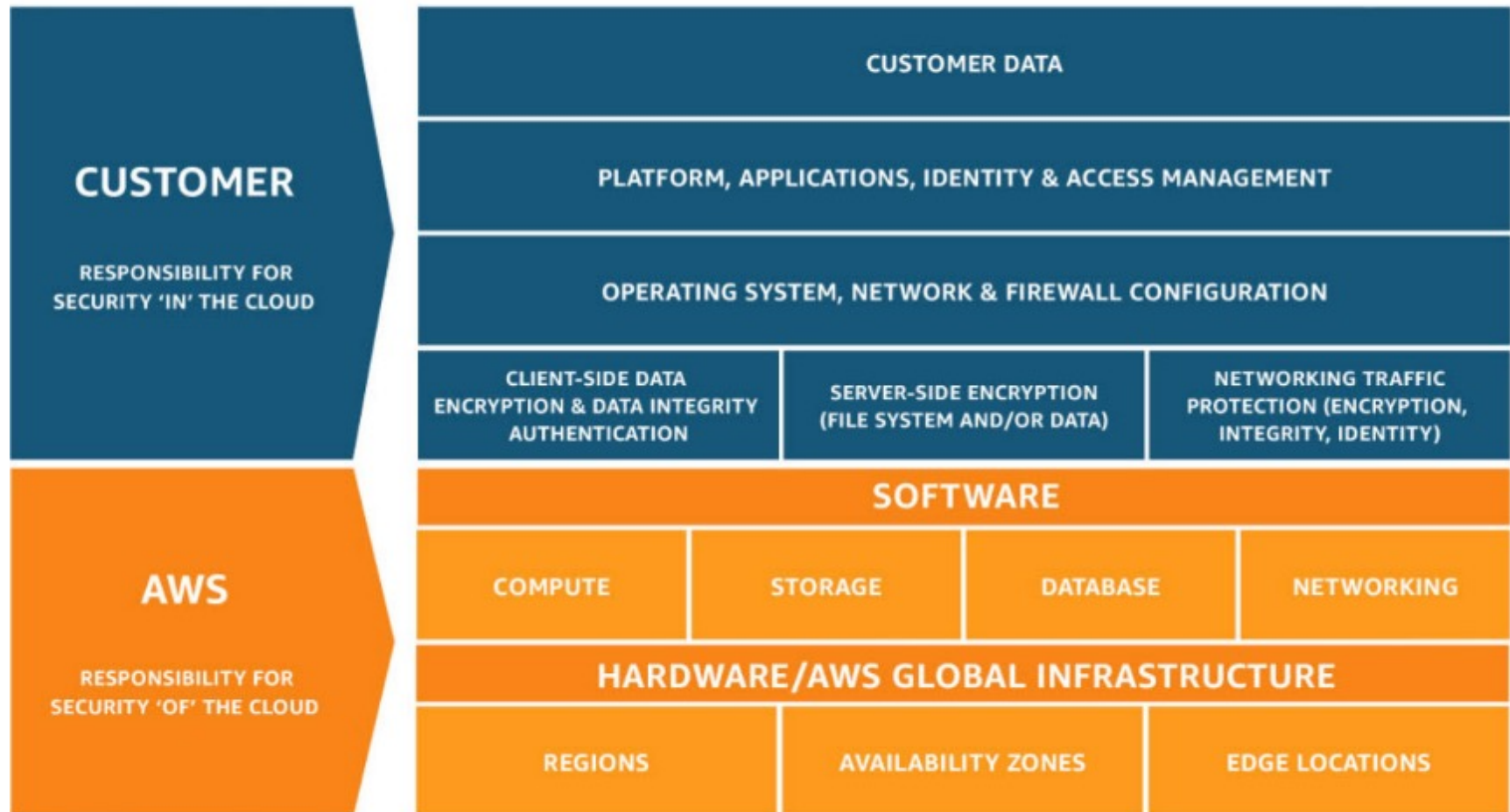
Microsoft Cloud Adoption Framework for Azure



Define Clearly The Responsibilities

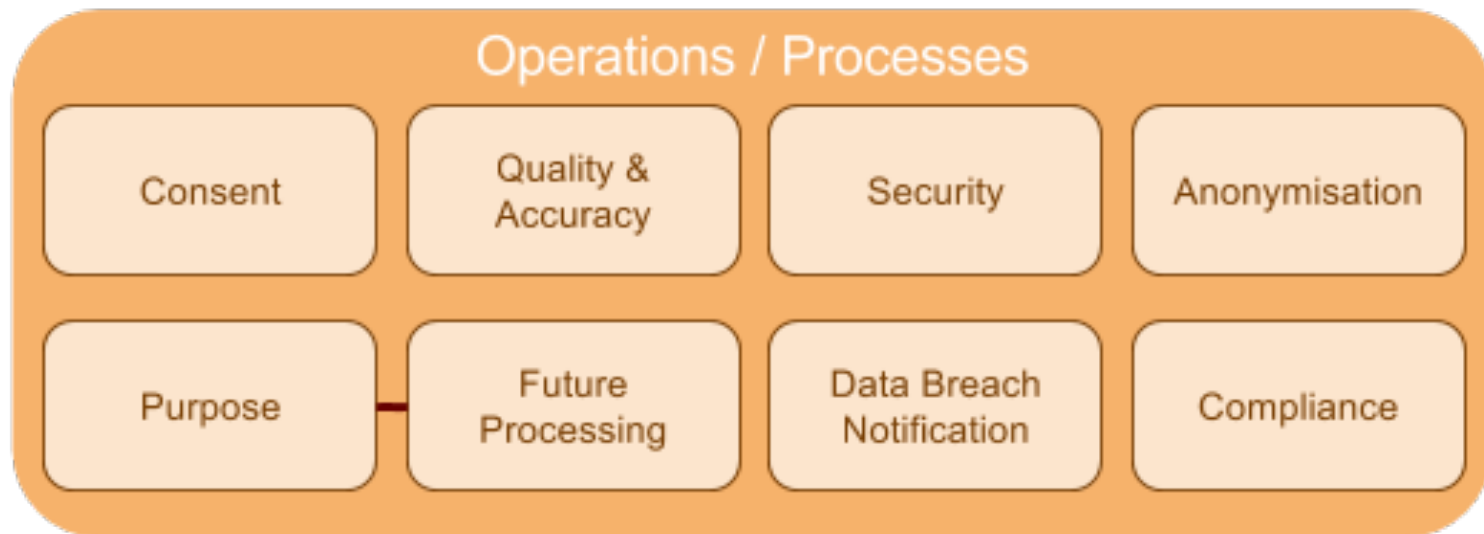


Example: AWS Cloud Security





Process failure = compliance failure





GDPR Definition: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her

Art. 7 GDPR

Conditions for consent

1. Where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.
2. ¹ If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. ² Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding.
3. ¹ The data subject shall have the right to withdraw his or her consent at any time. ² The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. ³ Prior to giving consent, the data subject shall be informed thereof. ⁴ It shall be as easy to withdraw as to give consent.
4. When assessing whether consent is freely given, utmost account shall be taken of whether, *inter alia*, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.





Name and surname: Maria Rodriguez
Address: 123 Maple Street, Apartment 4B,
Springfield, IL 62704
Reason for visit: Type 2 Diabetes and
hypertension
Healthcare Institution: Community Health
Partners Medical Center



Name and surname: <empty>
Address: <empty>
Reason for visit: Type 2 Diabetes and
hypertension
Healthcare Institution: Community Health
Partners Medical Center

Age	Zip	Gender	Diagnosis
23	10001	Male	Flu
27	10012	Female	Asthma
25	10007	Female	Diabetes
43	20001	Male	Hypertension



Age	Zip	Gender	Diagnosis
20-30	100*	Male	Flu
20-30	100*	Female	Asthma
20-30	100*	Female	Diabetes
40-50	200*	Male	Hypertension



Who notifies? The cloud provider or the customer? What if the provider discovers breach after 72h?

Art. 33 GDPR

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with [Article 55](#), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. ²Where the notification to the supervisory authority is not made **within 72 hours**, it shall be accompanied by reasons for the delay.
2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
3. The notification referred to in paragraph 1 shall at least:
 - a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
 - c) describe the likely consequences of the personal data breach;
 - d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.



Process of complying with cloud usage regulatory standards as well as local, national, and international laws

Governance & Accountability

- Know Your Shared Responsibility Model
- Document Controls and Evidence
- Conduct Regular Audits & Assessments
- Train Your Team Continuously

Security & Access Control

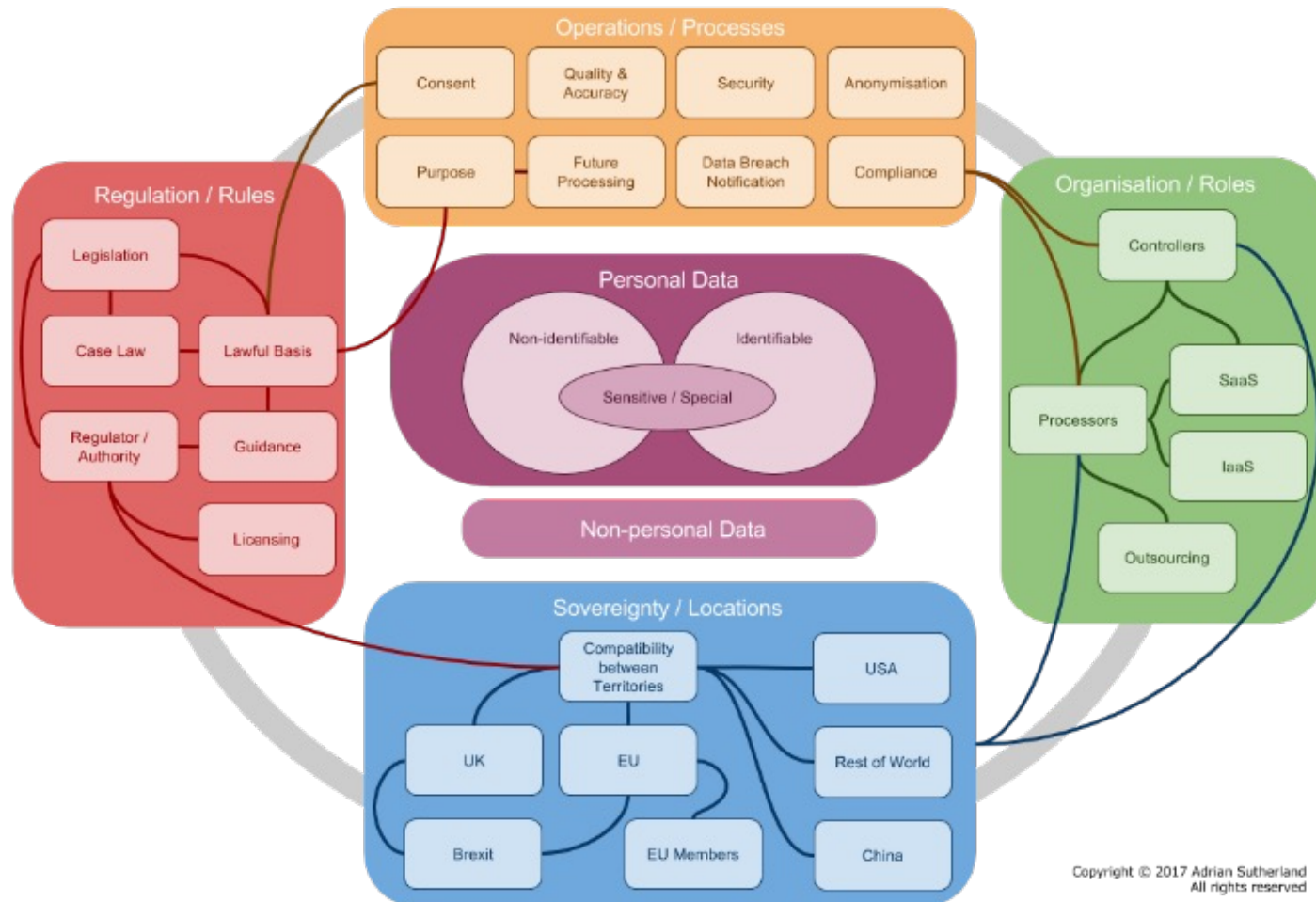
- Segment and Isolate Environments
- Implement Identity & Access Management (IAM) Strictly
- Encrypt Data Everywhere

Operating and Monitoring

- Automate Compliance with Policy-as-Code
- Enable Comprehensive Logging & Monitoring
- Maintain Continuous Monitoring & Logging
- Develop a Robust Incident Response Plan for Cloud



Can we demonstrate control, compliance, and accountability at any time?



Copyright © 2017 Adrian Sutherland
All rights reserved

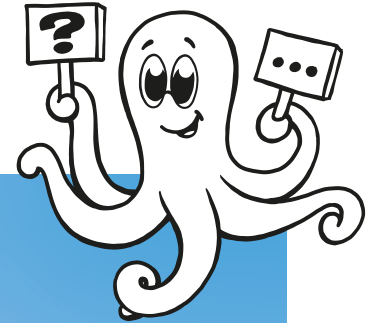


TOP 3 DATA PROTECTION CONCERNS FOR CLOUD COMPUTING

- 1 Lack of control over the data 82%
- 2 Increase vulnerabilities from shared infrastructure 79%
- 3 Privileged user abuse at Cloud provider 77%



Harnessing the benefits of cloud technologies, safeguarding personal data and meeting regulatory requirements



Which Journey to the Cloud?



No “one-size-fits-all”





The 6 Rs by Stephen Orban

- 1. Rehost** – “Lift-and-shift”
Move applications as-is to the cloud. Fast, low-risk, but may not optimize costs or performance.
- 2. Replatform** – “Lift-tinker-and-shift”
Make minor optimizations (e.g., upgrade database, adjust OS) during migration to gain some cloud benefits without major redesign.
- 3. Refactor / Rearchitect**
Redesign the application to be cloud-native (e.g., microservices, serverless). Maximizes scalability and cost savings but is time-intensive.
- 4. Repurchase** – “Drop-and-shop”
Switch to a different product, often moving to a SaaS platform (e.g., from on-prem CRM to Salesforce).
- 5. Retire**
Identify and decommission applications that are no longer useful or needed.
- 6. Retain (or Revisit)**
Keep some applications on-premises, often due to compliance, legacy dependencies, or short-term timelines.



1. **Assessment phase:** Understanding your current infrastructure

Before considering cloud migration, it's imperative to thoroughly assess your current IT environment. This involves cataloging your applications, data, and workloads and evaluating their readiness and suitability for a cloud-based infrastructure. During this phase, identify potential benefits, costs, compliance needs, and technical or business challenges.

1. **Planning phase:** Strategy, objectives, and cloud deployment model

In the planning phase, you will define the scope of your migration. It includes selecting the cloud deployment Model that aligns with your business needs -public, private, hybrid, or multi-cloud - and the strategy for the move, be it rehosting, replatforming, rearchitecting, or a combination thereof. This phase also involves building a detailed cloud migration checklist and process plan, setting clear objectives, and establishing a timeline.

3. **Proof of concept:** Testing the migration approach

A proof of concept (PoC) is a critical intermediate step that allows you to test your migration strategy on a small scale. This helps validate the approach and make necessary adjustments before full-scale execution, reducing risks and ensuring that your plan is robust.

4. **Migration execution:** Applying the "6Rs" strategies

This is where the actual migration happens. Execute the migration according to the chosen strategy, be it one of the "6Rs" or a custom approach. Ensure that your migration is supported by appropriate enterprise architecture tools and resources for a smooth transition.

5. **Validation and testing:** Ensuring performance and security

Once the migration is underway or completed, it is crucial to validate the performance and security of your applications in the cloud setup. Test to confirm that all systems operate correctly and meet predefined performance benchmarks.

6. **Optimization:** Fine-tuning for efficiency and cost-effectiveness

Post-migration, focus on optimizing your cloud resources. This involves continuous monitoring, cost management, performance tuning, and leveraging cloud-native features for improved efficiency and alignment with business goals.

7. **Operational handover:** Transitioning to ongoing management

The final phase is the operational handover, where the day-to-day management of the cloud infrastructure is transitioned to operational teams. This includes setting up a governance framework, ensuring proper staff training, and establishing operational best practices for the new cloud environment.

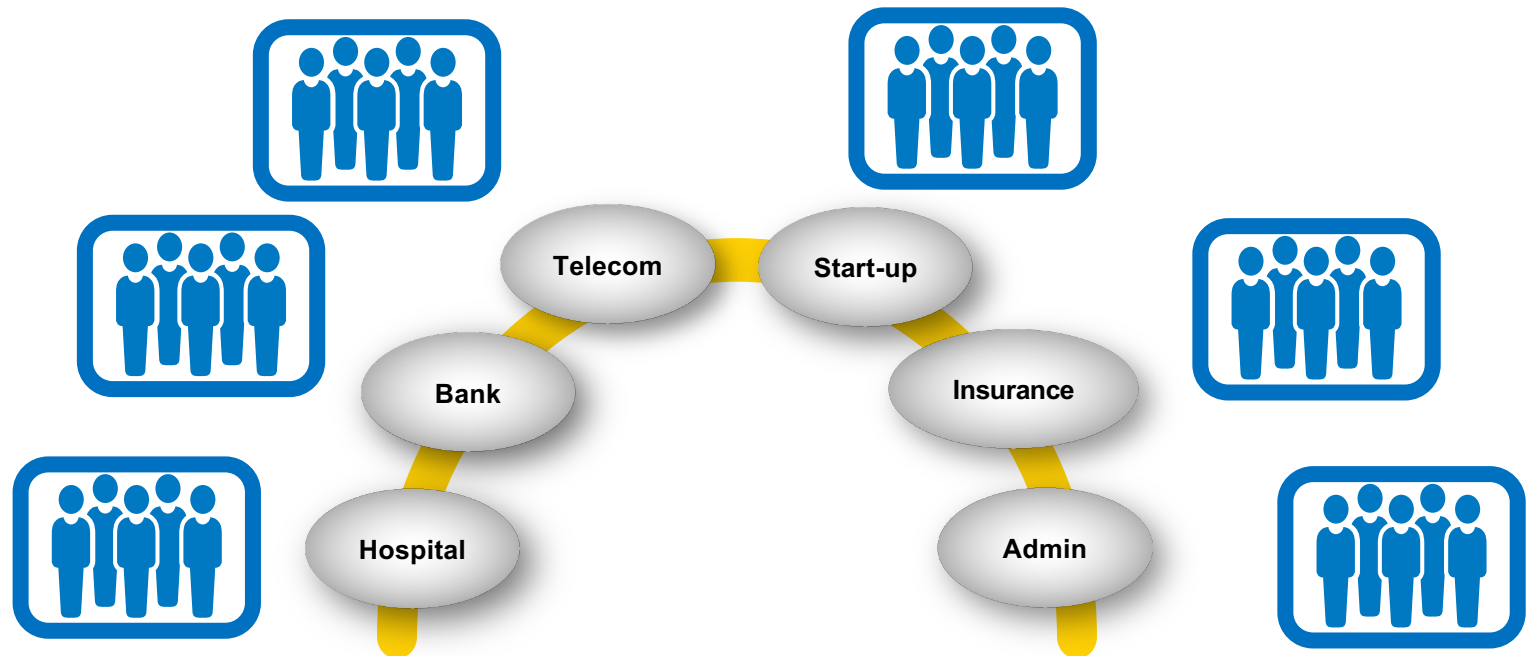


Which Journey to the Cloud?



Please define the way to the Cloud for the following organizations

1. Hospital
2. Bank
3. Telecom Company
4. Start-up
5. Insurance
6. Public Administration

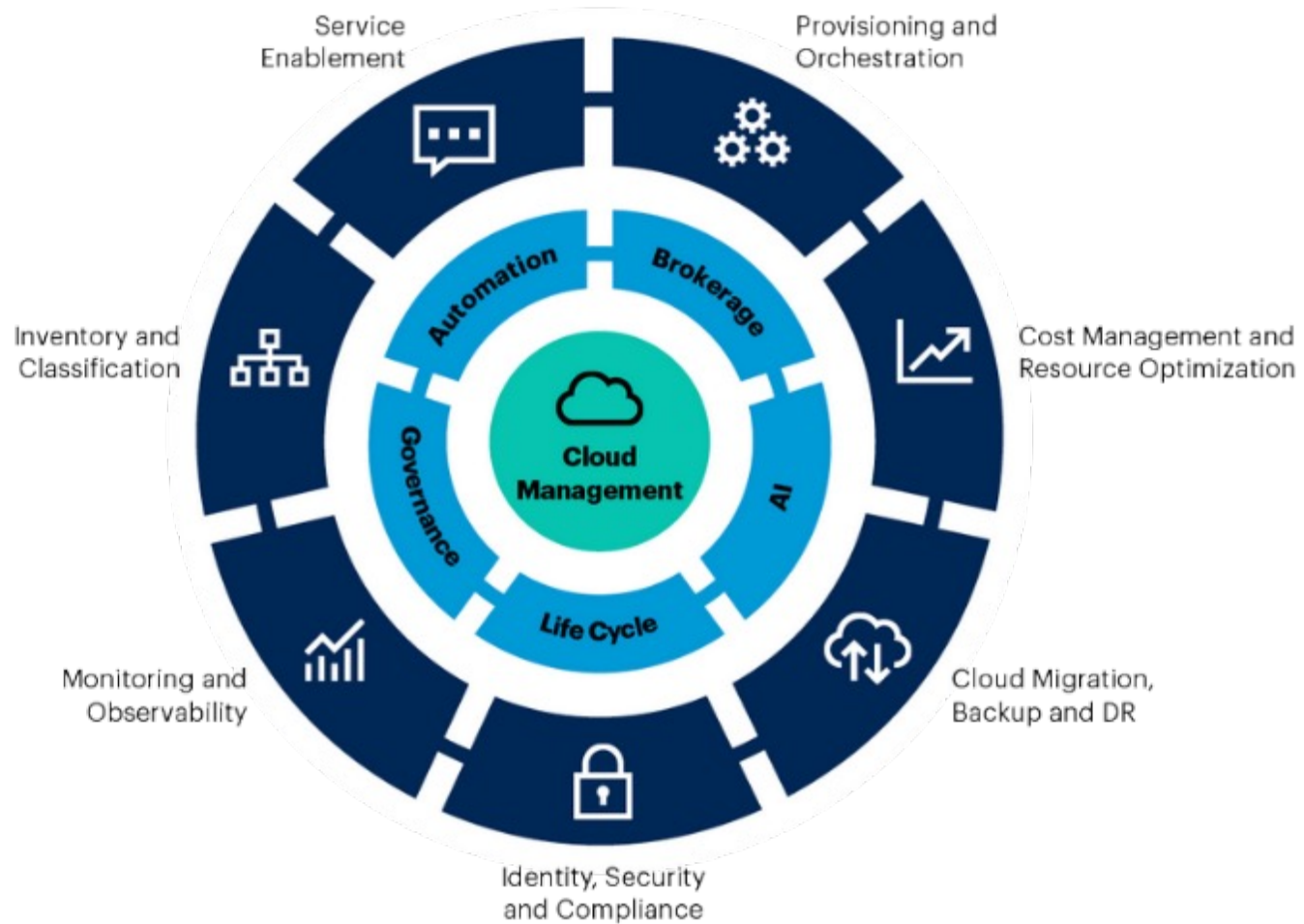


Balancing Agility, Cost, and Control in the Cloud





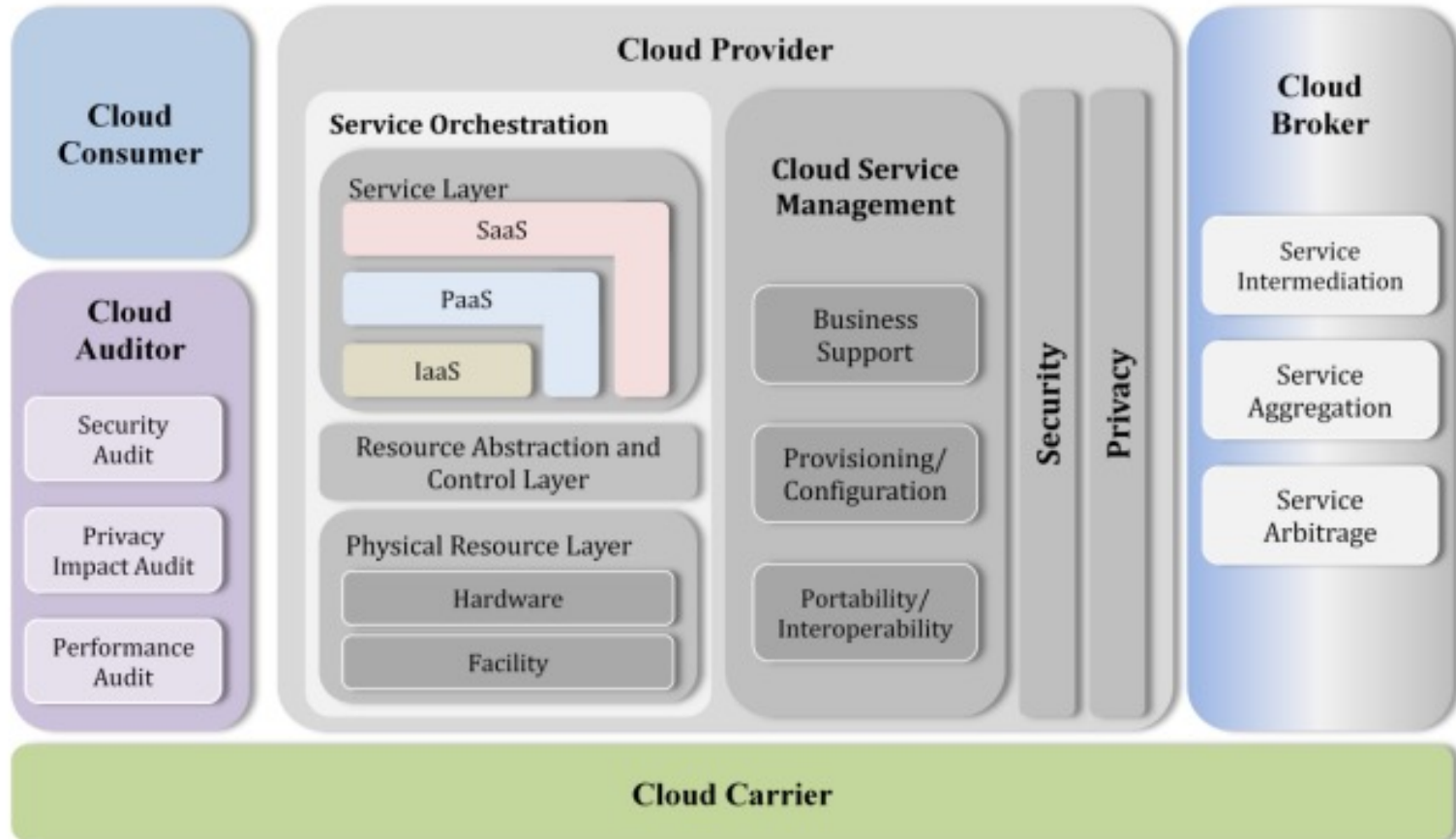
The Areas of Cloud Management



Source: Gartner
465209_C



NIST Cloud Computing Reference



NIST: National Institute of Standards and Technology



- **Security & Access Control:** Defining who can access what data, enforcing encryption, and monitoring for anomalies, often integrating with cloud IAM systems.
- **Data Quality & Integrity:** Ensuring data is accurate, consistent, and complete through validation and monitoring, even as it moves across platforms.
- **Compliance & Risk Management:** Meeting legal/regulatory needs (like GDPR) with policies for retention, archival, and data lineage.
- **Metadata Management:** Using tags and catalogs to add context, classify data (e.g., sensitive), and track it across its lifecycle.
- **Data Discovery & Lineage:** Knowing where data resides, how it flows, and its origins.
- **Auditing & Monitoring:** Regularly reviewing controls & tracking data usage (detect anomalies)



- IAM: Identity and Access Management
- GDPR: General Data Protection Regulation



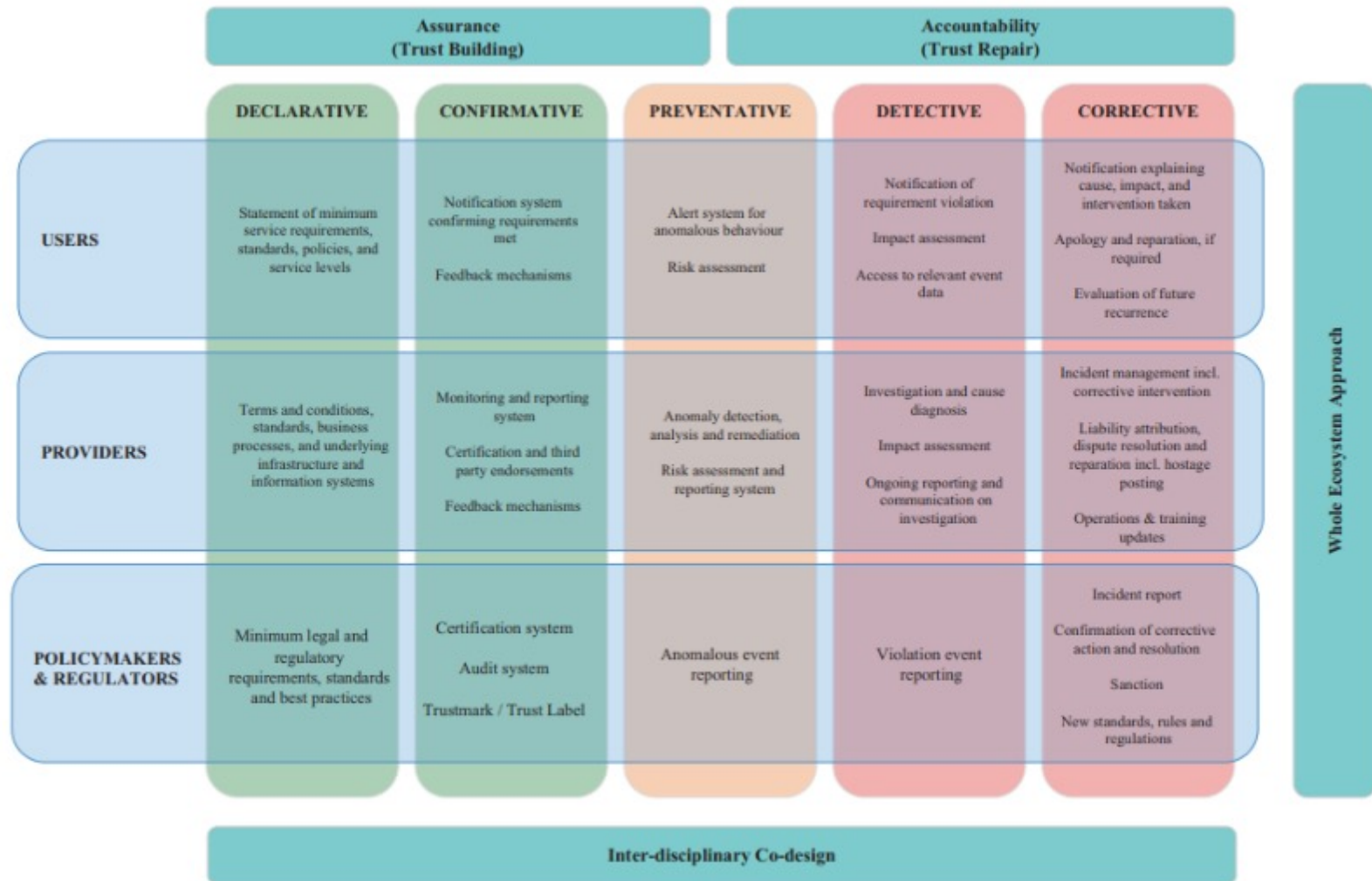
It is composed of 197 control objectives that are structured in 17 domains covering all key aspects of cloud technology. It can be used as a tool for the systematic assessment of a cloud implementation and provides guidance on which security controls should be implemented by which actor within the cloud supply chain.

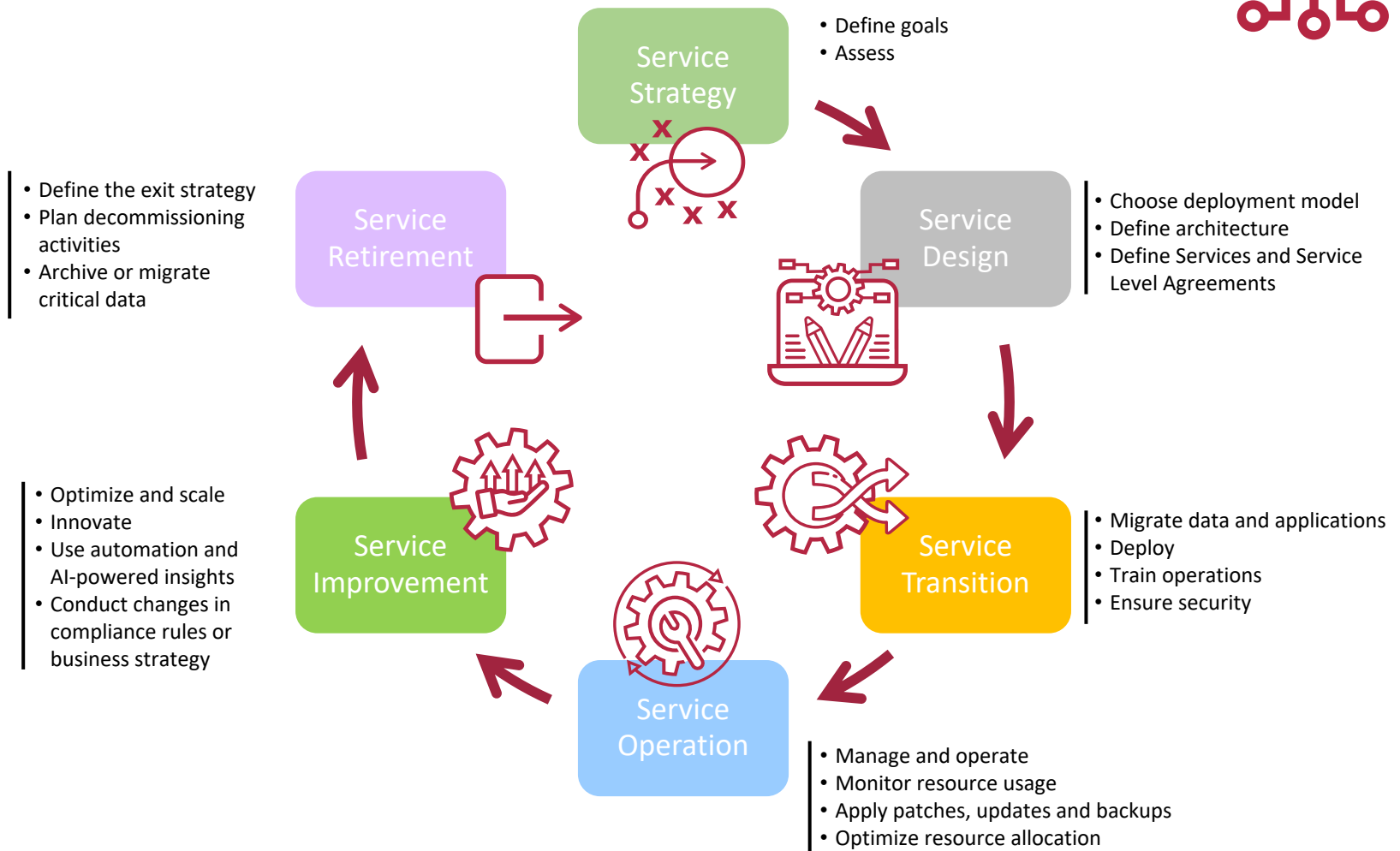
A&A	Audit & Assurance	IAM	Identity & Access Management
AIS	Application & Interface Security	IPY	Interoperability & Portability
BCR	Business Continuity Mgmt & Op Resilience	IVS	Infrastructure & Virtualization Security
CCC	Change Control & Configuration Management	LOG	Logging & Monitoring
CEK	Cryptography, Encryption, & Key Management	SEF	Sec. Incident Mgmt, E-Disc & Cloud Forensics
DCS	Datacenter Security	STA	Supply Chain Mgmt, Transparency, & Accountability
DSP	Data Security & Privacy	TVM	Threat & Vulnerability Management
GRC	Governance, Risk Management, & Compliance	UEM	Universal Endpoint Management
HRS	Human Resources Security		

Building and Maintaining Trust



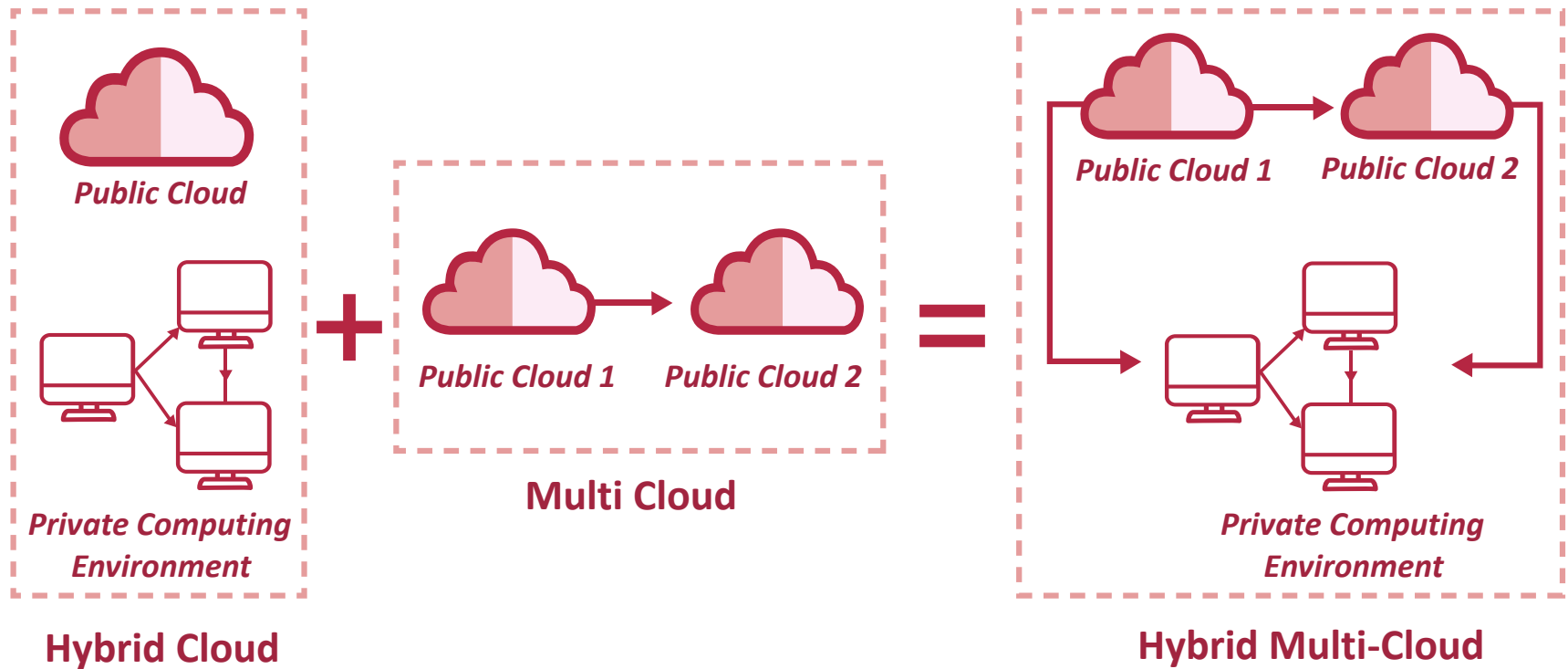
Trust must be demonstrated







Complexity vs flexibility trade-off





Cloud transformation is a company-wide change, not just a technical migration



Core Pillars of Cloud Transformation

1. Business Innovation

Using cloud capabilities (AI/ML, IoT, big data) to create new services, improve CX, enter new markets

2. Technology Modernization

Cloud-native architectures (microservices, serverless, containers), DevOps, data platforms

3. Process & Operating Model Change

Agile at scale, product-centric teams, platform-based delivery, FinOps

4. People & Culture

Upskilling, new collaboration models, fail-fast mindset, decentralized ownership



A retail company doing **cloudification** moves its on-prem servers and ERP to AWS to reduce data centre costs.

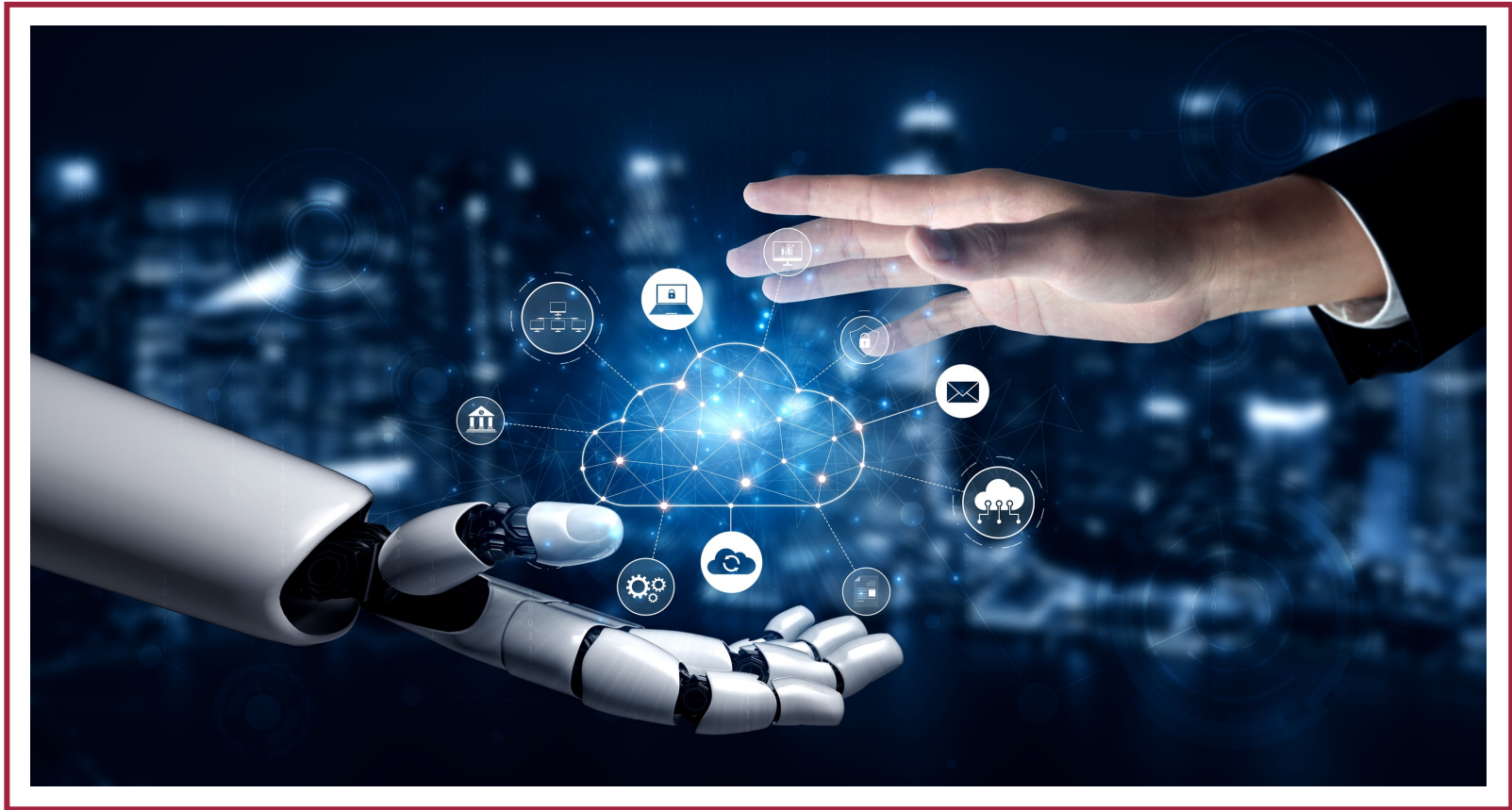
The same company doing **cloud transformation**:

- Uses cloud AI for personalized real-time recommendations.
- Develops a mobile app with serverless backend for omnichannel shopping.
- Empowers store associates with cloud-based inventory tools.
- Creates a data platform that merges online/offline behaviour to drive dynamic pricing.
- Adopts agile product teams where marketing, IT, and ops collaborate continuously.

The Future of Cloud Computing



From infrastructure → platforms → autonomous, invisible systems



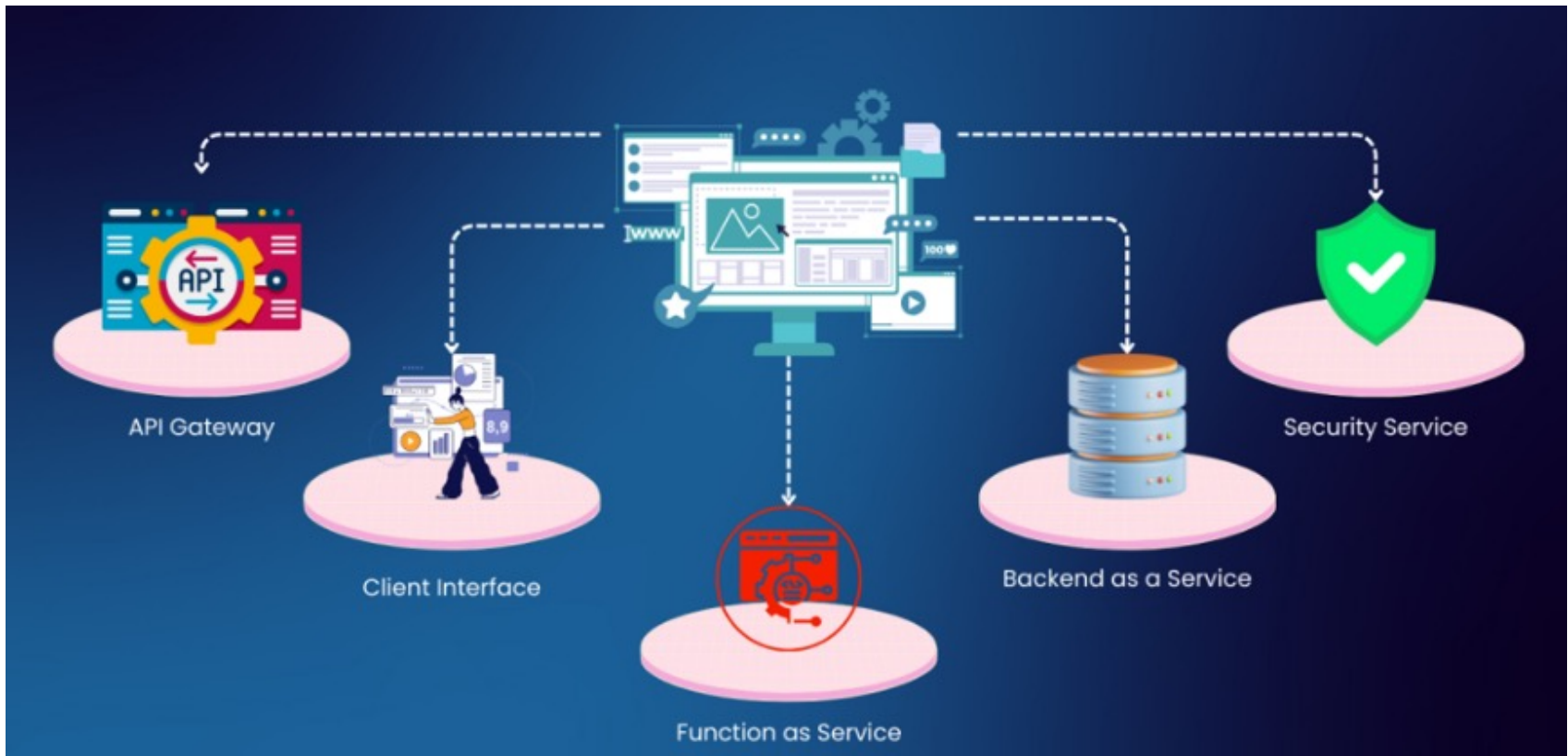


A single cloud platform running across central cloud regions, edge locations and on-premises data centers





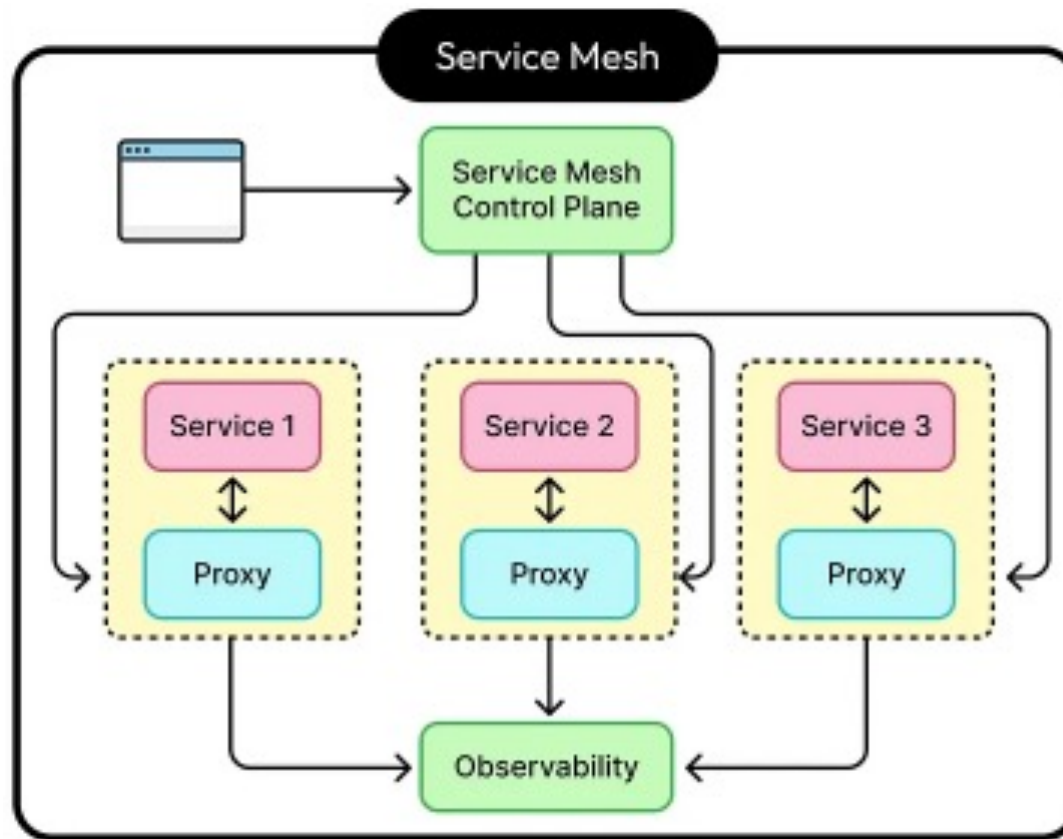
Deployment of functions or managed services as Functions-as-a-Service (FaaS) where every cloud service (databases, messaging, analytics, AI) is consumption-based and completely managed



- API: Application Programming Interface



Moving communication, security, and observability from applications into the platform





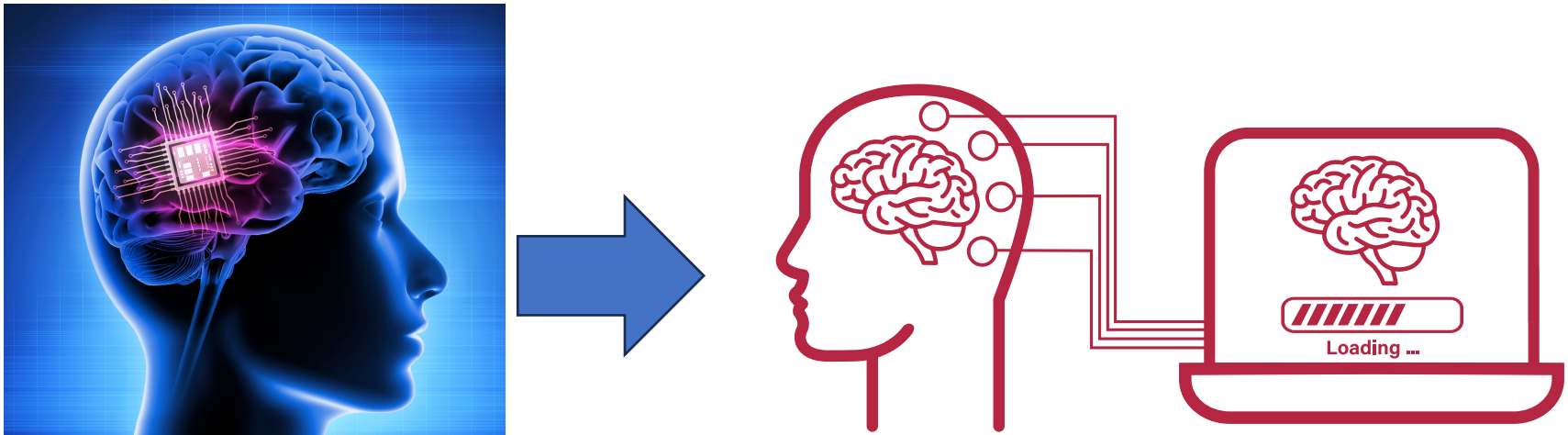
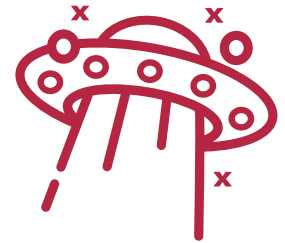
A hidden control layer coordinates secure, real-time interaction between distributed components



Beyond Cloud: When Computing Becomes Invisible and Internal

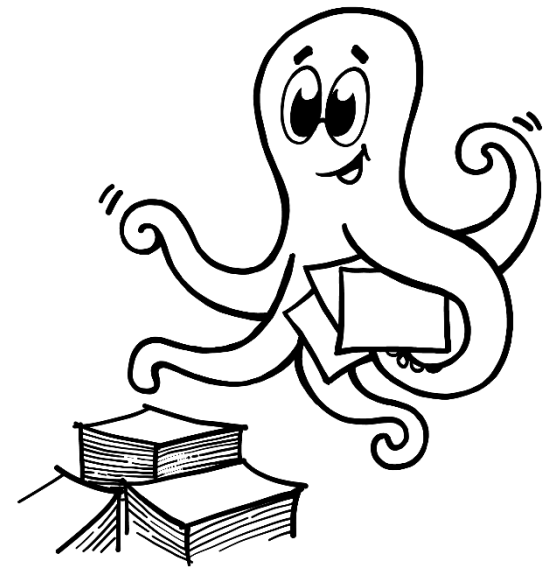


From Brain–Computer Interfaces (BCI) to the idea of “Mind Uploading”



- **Data ownership & mental privacy:** Who owns brain-generated data—and can thoughts be protected as personal data under frameworks such as the General Data Protection Regulation?
- **Consent & autonomy:** How can individuals give informed consent if data is captured directly from neural activity, potentially without full awareness or control?
- **Personhood, jurisdiction & control:** If mind uploading became possible, would a cloud-based simulation of a human mind have legal personhood? Who has the right to delete it, copy it, or modify it? Which jurisdiction applies if it is distributed across global cloud infrastructure?

- To understand the different kinds of Cloud
- To know the advantages of Cloud and also the challenges
- To know the key elements of the Cloud Data Protection Framework
- To be able to draw a roadmap for the journey to the Cloud
- To show the different steps concerning the Cloud Service Lifecycle



- BSI (2011) Security Recommendations for Cloud Computing Providers. Elsevier Ltd
- Datenschutzbeauftragten des Bundes und der Länder (2014) Orientierungshilfe – Cloud Computing.
- Liu F., Tong J., Mao J., Bohn R. , Messina J., Badger L., Leaf D. (2023) NIST Cloud Computing Reference Architecture. NIST Special Publication 500-292
- Lynn T., Mooney J.G. (2021) Data Privacy and Trust in Cloud Computing. Palgrave Studies





KNOWLEDGE