CYBER SECURITY AND BUSINESS CONTINUITY

INDUSTRIENS FOND SDU FORSVARSAKADEMIET

Digitalisation and Cloud Computing

Marco Peressotti

Department of Mathematics and
Computer Science
University of Southern Denmark

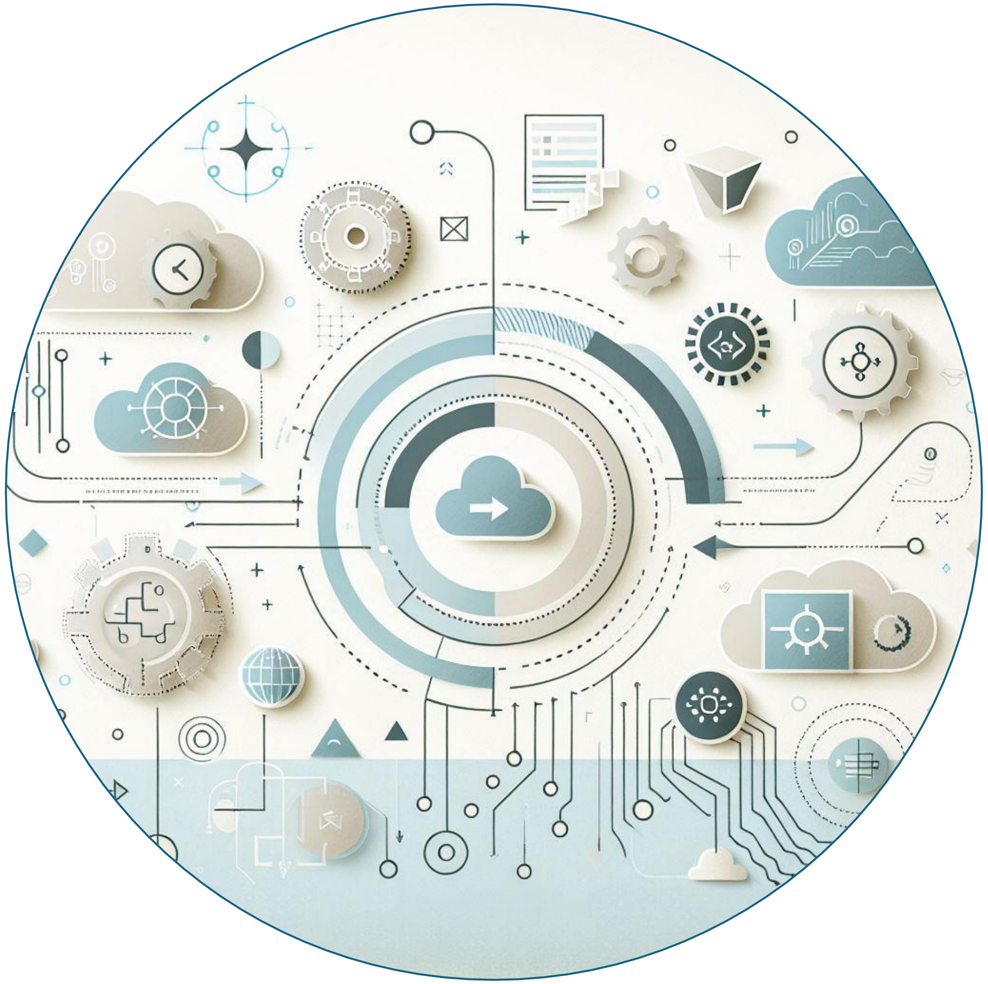
marcoperessotti.com

What is Digitalisation?

Definition: Digitalisation is the integration of digital technologies into everyday business processes, fundamentally changing how businesses operate and deliver value to customers.

Key Aspects:

- **Automation of Processes**: e.g., automating invoice processing to reduce manual errors and speed up payment cycles.
- **Data-Driven Decision-Making**: e.g., using data analytics to predict market trends and customer preferences.
- **Enhanced Customer Experiences**: e.g.,: implementing chatbots for 24/7 customer support.



Benefits of Digitalization

- **Operational Efficiency**: Improved logistics and supply chain management.
  - Using RFID tags to track equipment and supplies in real-time.
  - A business using cloud-based inventory management to reduce overstock and stockouts.
- **Real-Time Data**: Better decision-making with real-time data analytics.
  - A manufacturing company using IoT sensors to monitor equipment health and schedule maintenance proactively.
- **Collaboration**: Improved communication and collaboration across teams and with partners.
  - Using a secure cloud-based platform for joint operations planning and execution.
- **Enhanced Security**: Advanced cybersecurity measures to protect sensitive data.
  - Implementing a zero-trust security model to ensure only authorized personnel can access critical systems.

Key Technologies

- **Cloud Computing**: Scalable and flexible IT resources.
  - Using a cloud-based ERP system to streamline supply chain management and production processes.
  - Using cloud storage to securely share critical documents with authorized personnel.
- **Internet of Things (IoT)**: Connected devices for real-time monitoring and control.
  - Using IoT sensors to monitor equipment and schedule maintenance proactively.
- **Artificial Intelligence (AI)**: Intelligent automation and data analysis.
  - Using AI to enhance quality control by detecting defects in manufactured components.
- **Big Data Analytics**: Insights from large volumes of data.
  - Analyse product telemetry and improve offerings.
  - Analyse production and demand to optimise inventory levels and forecast demand.

What is Cloud Computing?

What is Cloud Computing?

Definition: a model for 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.

NIST

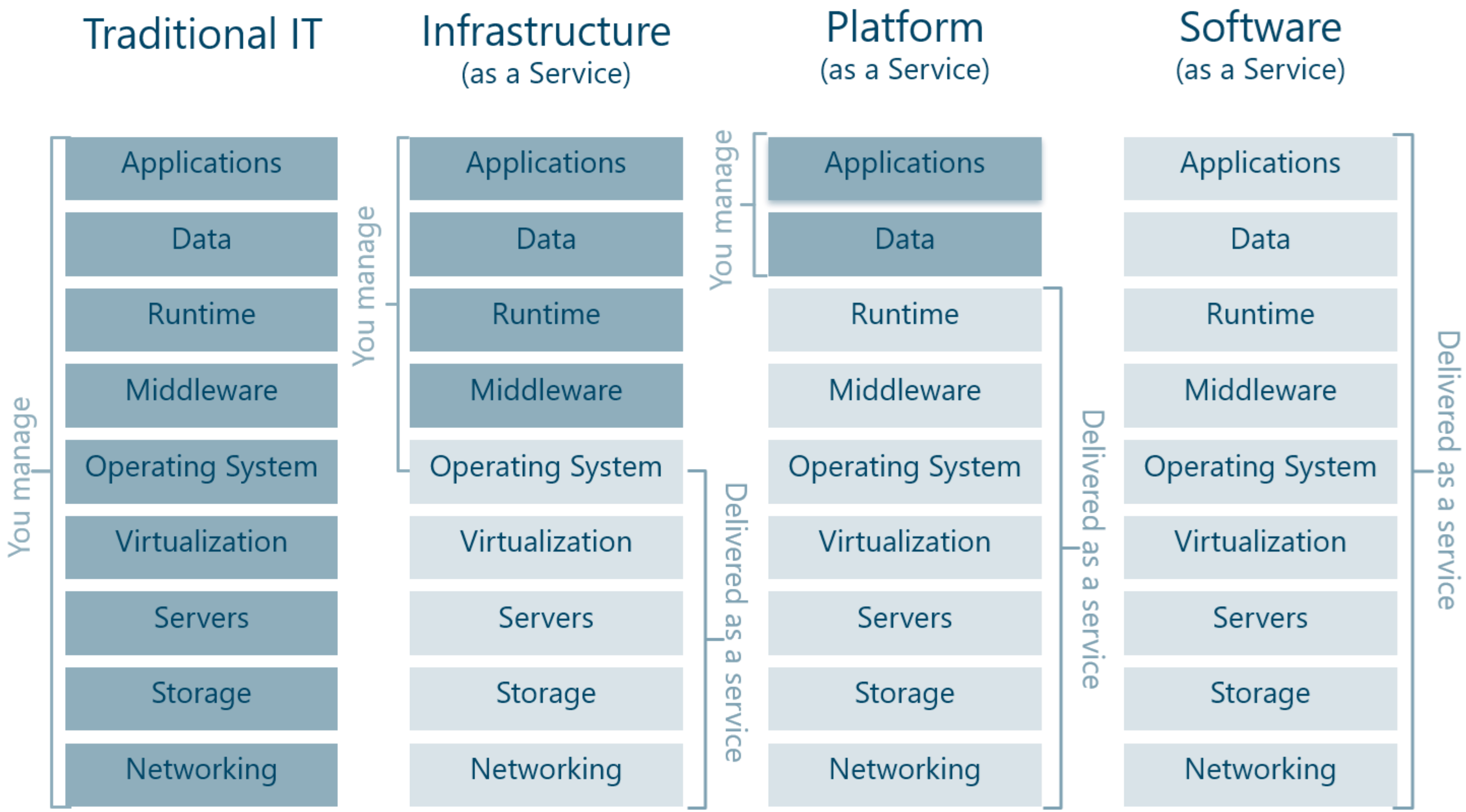
What is Cloud Computing?

Definition: a model for 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.

NIST

- **On-demand self-service:** Cloud resources can be accessed or provisioned without human interaction.
- **Broad network access**: Users can access cloud services and resources through any device and network provided that they have permission.
- **Resource pooling**: Cloud provider resources are shared by multiple tenants while keeping the data of individual clients inaccessible for other clients.
- **Rapid elasticity**: Unlike on-premise hardware and software, cloud computing resources can be rapidly increased or decreased to meet clients' changing needs.
- **Measured service**: Usage of cloud resources is metered so that businesses and other cloud users need only pay for the resources they use in any given billing cycle.

Cloud Delivery Models



Traditional IT

You manage

Applications
Data
Runtime
Middleware
Operating System
Virtualization
Servers
Storage
Networking

Infrastructure
(as a Service)

You manage

Applications
Data
Runtime
Middleware

Delivered as a service

Operating System
Virtualization
Servers
Storage
Networking

Platform
(as a Service)

You manage

Applications
Data

Delivered as a service

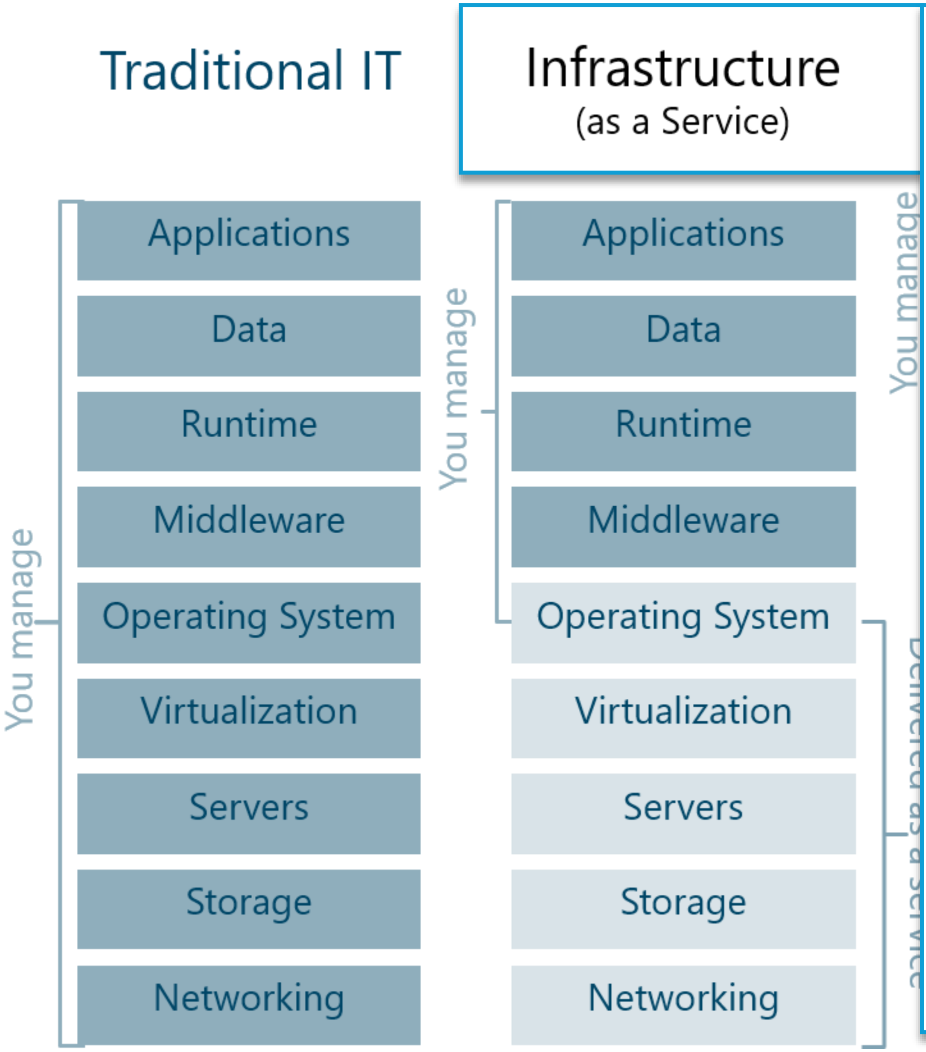
Runtime
Middleware
Operating System
Virtualization
Servers
Storage
Networking

Software
(as a Service)

Delivered as a service

Applications
Data
Runtime
Middleware
Operating System
Virtualization
Servers
Storage
Networking

Cloud Delivery Models



Provides virtualised computing resources over the internet.

Key Features:

- Virtual machines and storage
- Networking capabilities
- Load balancers
- Example Providers: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP)

Use Cases:

- Hosting websites and applications
- Data storage and backup
- Disaster recovery solutions

Cloud Delivery Models

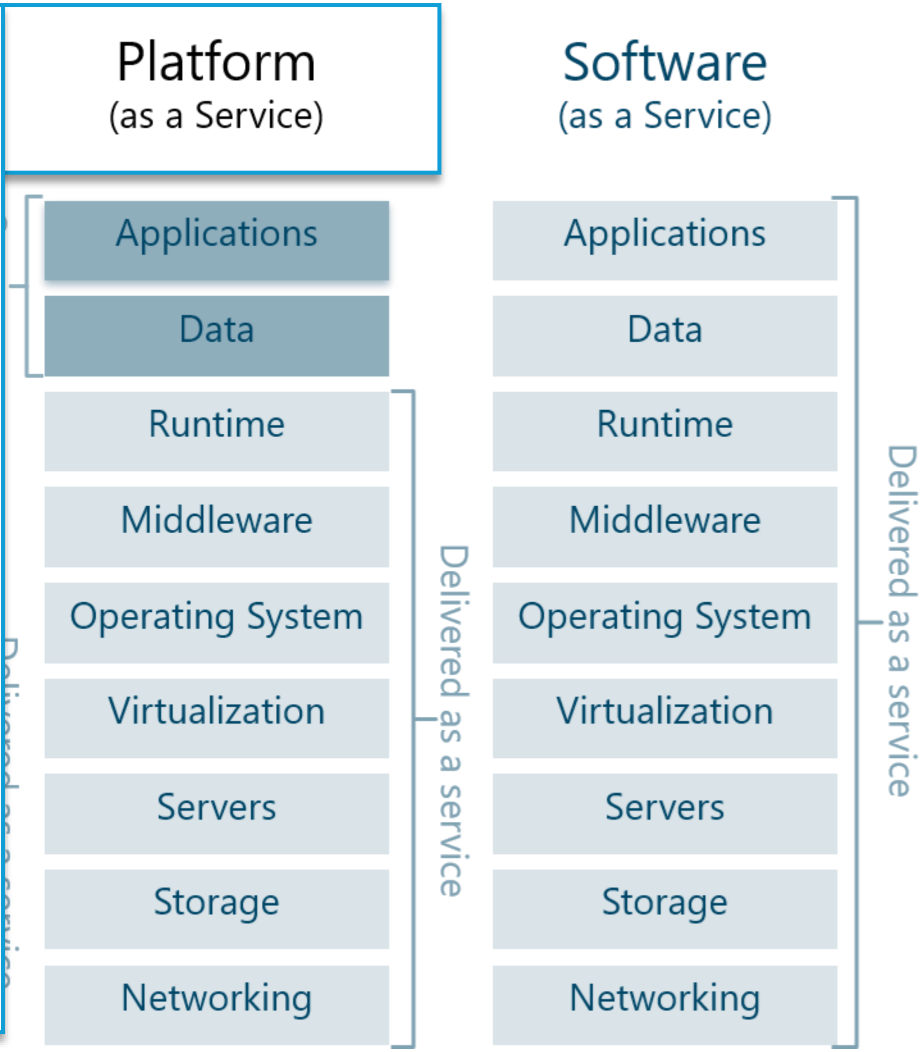
Offers hardware and software tools over the internet.

Key Features:

- Development frameworks
- Middleware
- Database management systems
- Example Providers: Google App Engine, Heroku, Microsoft Azure App Services

Use Cases:

- Developing, testing, and deploying applications
- Streamlining development workflows
- Managing application lifecycle



Platform (as a Service)	Software (as a Service)
Applications	Applications
Data	Data
Runtime	Runtime
Middleware	Middleware
Operating System	Operating System
Virtualization	Virtualization
Servers	Servers
Storage	Storage
Networking	Networking

Delivered as a service

Delivered as a service

Cloud Delivery Models

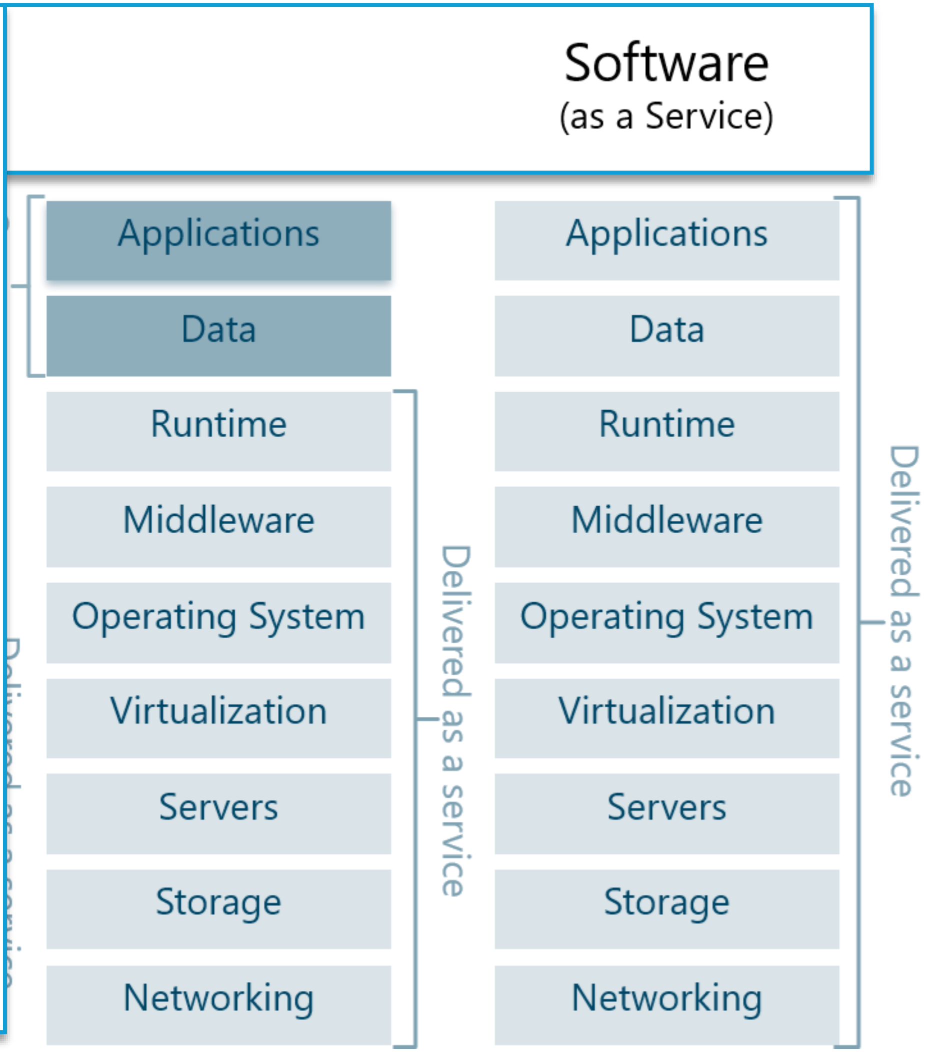
Delivers software applications over the internet, on a subscription basis.

Key Features:

- Web-based access to software
- Automatic updates and patch management
- Multi-tenancy model
- Example Providers: Google Workspace, Microsoft 365, Salesforce

Use Cases:

- Email and collaboration tools
- Customer relationship management (CRM)
- Enterprise resource planning (ERP)

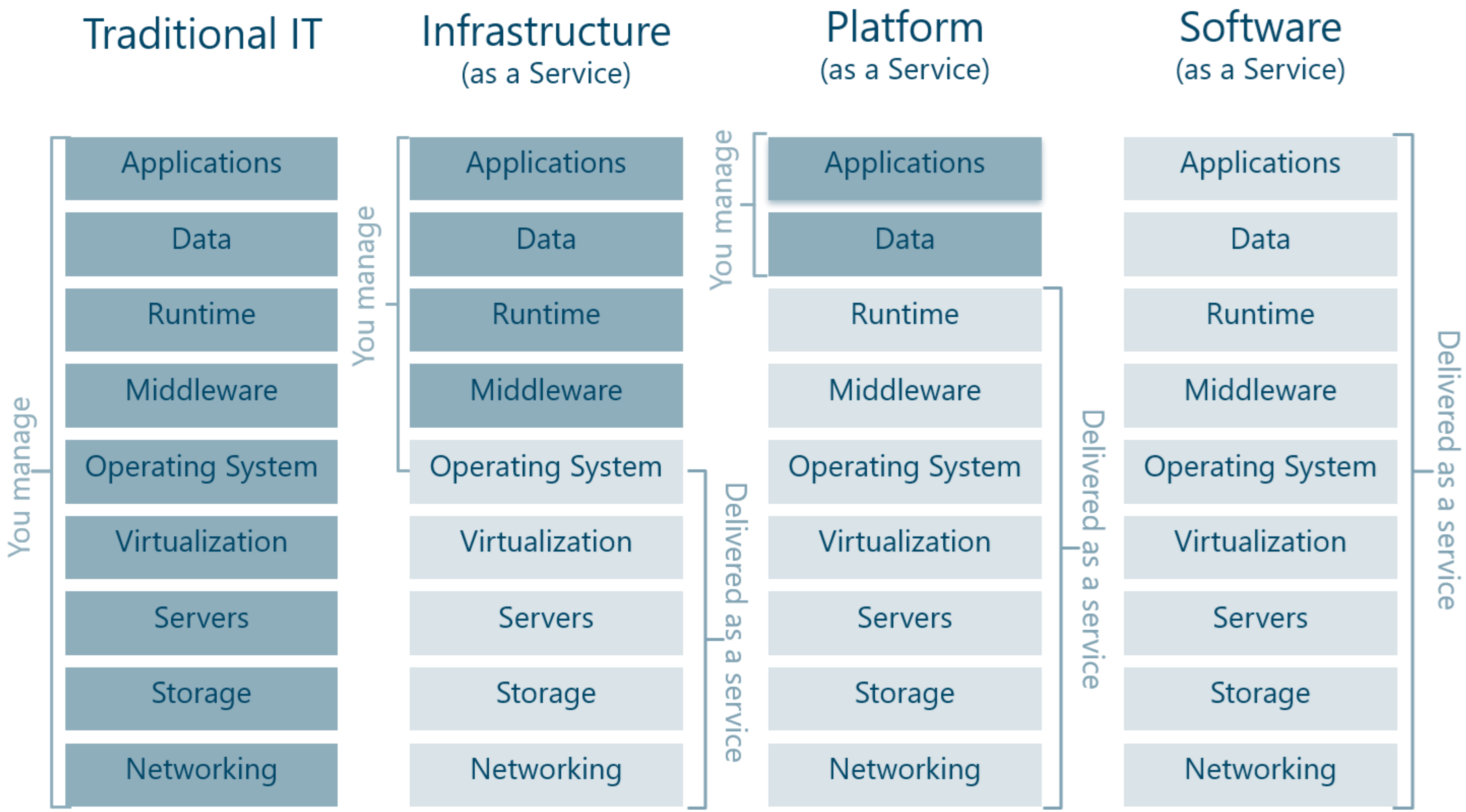


Software
(as a Service)

Applications
Data
Runtime
Middleware
Operating System
Virtualization
Servers
Storage
Networking
Delivered as a service

Applications
Data
Runtime
Middleware
Operating System
Virtualization
Servers
Storage
Networking
Delivered as a service

Cloud Delivery Models



Traditional IT

You manage
- Applications
- Data
- Runtime
- Middleware
- Operating System
- Virtualization
- Servers
- Storage
- Networking

Infrastructure
(as a Service)

You manage
- Applications
- Data
- Runtime
- Middleware
- Operating System

Delivered as a service
- Virtualization
- Servers
- Storage
- Networking

Platform
(as a Service)

You manage
- Applications
- Data

Delivered as a service
- Runtime
- Middleware
- Operating System
- Virtualization
- Servers
- Storage
- Networking

Software
(as a Service)

Delivered as a service
- Applications
- Data
- Runtime
- Middleware
- Operating System
- Virtualization
- Servers
- Storage
- Networking

Cloud Environments

Public Cloud

Private Cloud

Hybrid Cloud

Multi Cloud

Cloud Environments

Public Cloud

Private Cloud

Hybrid Cloud

Multi Cloud

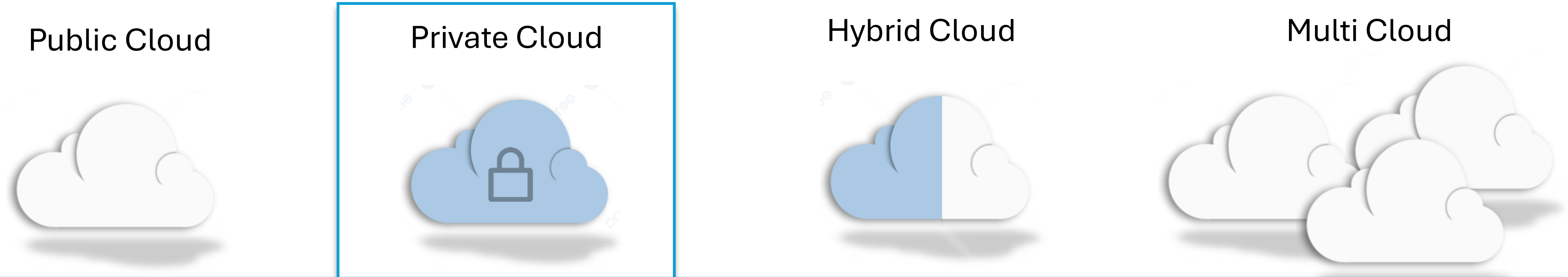
Services are delivered over the public internet and shared across multiple organisations.

Key Features:

- Cost-effective: Pay-as-you-go pricing model.
- Scalability: Easily scale resources up or down.
- Examples: Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP).

Use Cases: Ideal for non-sensitive data, development and testing environments, and high-volume applications.

Cloud Environments



Services are maintained on a private network and used exclusively by a single organisation.

Key Features:

- Enhanced Security: Greater control over data and security.
- Customization: Tailored to specific organisational needs.
- Examples: On-premises data centres, private cloud solutions from providers like VMware or OpenStack.

Use Cases: Suitable for sensitive data, critical applications, and organisations with strict compliance requirements.

Cloud Environments

Public Cloud

Private Cloud

Hybrid Cloud

Multi Cloud

Combines public and private clouds, allowing data and applications to be shared between them.

Key Features:

- Flexibility: Balance between cost-efficiency and security.
- Workload Optimization: Run workloads in the most appropriate environment.
- Examples: Integration of on-premises infrastructure with public cloud services.

Use Cases: Ideal for dynamic or highly changeable workloads, disaster recovery, and data backup.

Cloud Environments

Public Cloud

Private Cloud

Hybrid Cloud

Multi Cloud

Use of multiple cloud services from different providers.

Key Features:

- Avoid Vendor Lock-In: Flexibility to choose the best services from different providers.
- Redundancy: Increased reliability and availability.
- Examples: Using AWS for storage, Azure for computing, and Google Cloud for machine learning.

Use Cases: Organizations seeking to leverage the best features of various cloud providers and enhance redundancy.

Choosing Cloud Providers

Reliability and Performance:

- **Uptime**: Look for providers with a proven track record of high uptime (e.g., 99.9% or higher).
- **Performance Metrics**: Evaluate performance metrics such as latency, throughput, and response times.
- **Case Studies**: Review case studies or testimonials from other defence sector organizations.

Support and Service Level Agreements:

- **24/7 Support**: Ensure the provider offers round-the-clock support with quick response times.
- **SLAs**: Check the SLAs for guarantees on uptime, performance, and support response times.
- **Dedicated Account Management**: Look for providers that offer dedicated account managers for personalized support.

Compliance and Security:

- **Certifications**: Verify that the provider holds relevant security certifications (e.g., ISO/IEC 27001, NIST, GDPR).
- **Data Protection**: Ensure robust data protection measures, including encryption and access controls.
- **Audit Reports**: Request audit reports to review the provider’s security practices and compliance status.

Cost and Pricing Models:

- **Transparent Pricing**: Look for providers with clear and transparent pricing models.
- **Cost Predictability**: Evaluate options for fixed pricing or cost predictability to avoid unexpected expenses.
- **Total Cost of Ownership (TCO)**: TCO, including subscription fees, data transfer costs, etc.

Data Management

Data Storage

- **Redundancy**: Implement data redundancy to ensure data availability and reliability.
- **Tiered Storage**: Use tiered storage solutions to optimize cost and performance.
- **Encryption**: Encrypt data at rest to protect against unauthorized access.

Data Backup

- **Automated Backups**: Schedule automated backups to ensure regular and consistent data protection.
- **Offsite Storage**: Store backups in geographically diverse locations to protect against local disasters.
- **Testing**: Regularly test backup and recovery procedures to ensure they work as expected.

Data Recovery

- **Recovery Time Objectives (RTO)**: Determine acceptable downtime and recovery timelines.
- **Recovery Point Objectives (RPO)**: Specify the maximum acceptable data loss in terms of time.
- **Disaster Recovery Plans**: Develop, maintain, and exercise comprehensive disaster recovery procedures.

Data Governance

- **Policies and Procedures**: Establish clear data management policies and procedures.
- **Data Classification**: Classify data based on sensitivity and apply appropriate security controls.
- **Compliance**: Ensure compliance with relevant regulations and standards (e.g., GDPR, NIST, ISO/IEC 27001).

Data Recovery Plans

- **Cloud Service Inventory**: Identify all critical cloud services and their configurations and keep this inventory up to date.
- **Backup Strategy**: Perform continuous data replication, use multiple cloud regions to ensure redundancy, and encrypt all data in transit and at rest to protect against unauthorized access.
- **Recovery Procedures**: Define RTO and RPO, and outline step-by-step procedures for failing over, including reconfiguration and testing.
- **Testing and Maintenance**: Conduct regular failover tests to ensure recovery procedures work as expected and update the plan periodically to reflect changes.

Data Governance

Data Security Policy

- **Access Controls**: Implement role-based access controls (RBAC) to restrict data access based on user roles.
- **Encryption**: Encrypt sensitive data both in transit and at rest.
- **Incident Response**: Develop and maintain an incident response plan to address data breaches.

Data Classification Policy

- **Classification Levels**: Define levels such as public, internal, confidential, and restricted.
- **Labelling**: Label data according to its classification level.
- **Handling Procedures**: Establish procedures for handling data based on its classification.

Data Retention Policy

- **Retention Periods**: Specify retention periods for different types of data.
- **Archival**: Implement processes for archiving data that is no longer actively used but must be retained.
- **Deletion**: Ensure secure deletion of data that is no longer needed.

Data Access Policy

- **Access Requests**: Define procedures for requesting and granting access to data.
- **Audit Trails**: Maintain logs of data access and usage.
- **Review**: Regularly review access permissions to ensure they are up-to-date.

Shared Responsibility Model in Cloud Security

Cloud provider and user are both responsible for security, but the division of responsibilities varies depending on the cloud delivery model

	Infrastructure as a Service	**Platform as a Service**	**Service as a Service**
Provider	• Physical security of data centres • Infrastructure maintenance and security	• Physical security of data centres • Infrastructure and operating system maintenance and security	• Physical security of data centres • Entire infrastructure, operating system, and application
User	• Operating system management and security • Application security • Data management and protection • Compliance regulations	• Application security • Data management and protection • Compliance regulations	• Data management and protection • Compliance regulations

CYBER SECURITY AND BUSINESS CONTINUITY

INDUSTRIENS FOND SDU FORSVARSAKADEMIET

Digitalisation and Cloud Computing

Thank you for your attention.

Marco Peressotti

Department of Mathematics and
Computer Science
University of Southern Denmark

marcoperessotti.com