MODULE 6C: AUDITING CLOUD COMPUTING AND OUTSOURCE OPERATIONS

OBJECTIVES

- Definitions of cloud computing and other forms of IT outsourcing
- Third-party attestations and certifications, such as ISO 27001
- Vendor selection controls
- Items to include in vendor contracts
- Data security requirements
- Operational concerns
- Legal concerns and regulatory compliance

CLOUD COMPUTING

- Over the last couple of decades, the concept of *cloud computing* has brought outsourced IT to the mainstream by providing IT services over the Internet using shared infrastructure. Cloud computing has grown from its initial stages to an industry buzzword and now to a legitimate and powerful business and operations model.
- The National Institute of Standards and Technology (NIST) SP 800-145 defines cloud computing as “a model for enabling…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.”

CLOUD COMPUTING

- Basically, cloud computing provides IT services over the Internet in such a way that the end user doesn’t have to worry about where the data is being stored, where the infrastructure is located, and so on. The user receives the service without worrying about any of the details of how it’s provided. Typically, as a consumer of cloud computing, you are sharing the back-end infrastructure that provides the service with other *tenants*, including some of the provider’s other customers; it is not dedicated to you and your company.

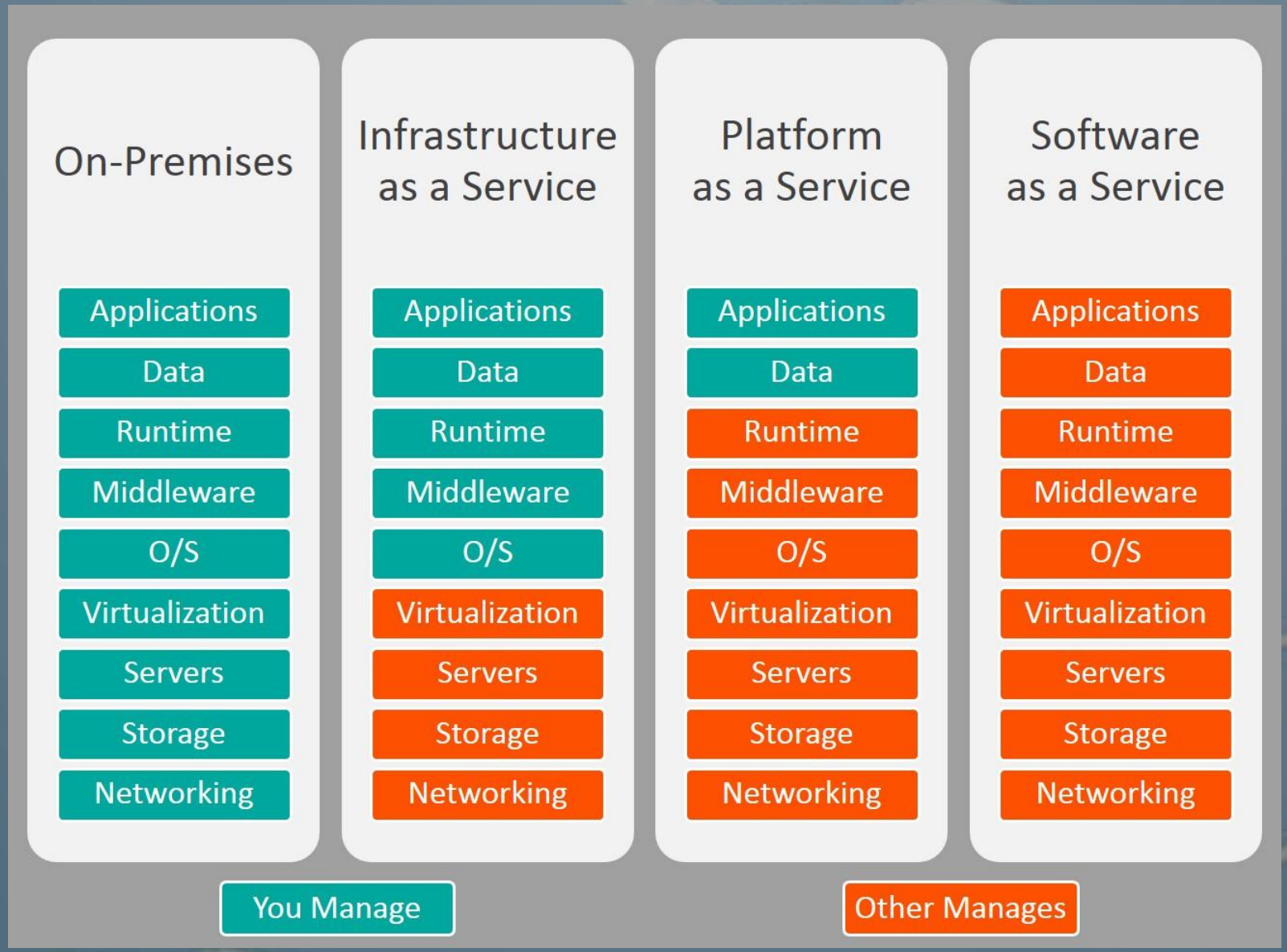
CLOUD COMPUTING

- Variety of Services:
  - Virtual client and server systems, allowing you to run Windows, Linux, or other operating systems in the provider's cloud environment
  - Storage platforms, such as Amazon S3, supporting general-purpose data storage
  - Serverless computing, allowing your code to run on the provider's infrastructure, freeing you from the overhead of supporting an underlying operating system
  - Databases, machine learning algorithms, and more

CHARACTERISTICS OF CLOUD COMPUTING

- **On-Demand Self-Service** This means that you can provision computing capabilities, such as storage, as needed automatically without requiring human interaction with each service's provider.
- **Broad Network Access** This means that capabilities should be accessible from anywhere and from any device (such as laptops and mobile devices) as long as Internet connectivity is available.
- **Resource Pooling** This means that the provider's computing resources are pooled to serve multiple consumers using a *multitenant* model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand, with separation of data and users accomplished through logical rather than physical means.
- **Rapid Elasticity** This means that capabilities can be rapidly and elastically provisioned (often automatically) to scale out quickly and rapidly released to scale in quickly. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be purchased in any quantity at any time.
- **Measured Service** This means that cloud systems automatically control and optimize resource usage by leveraging metering capabilities appropriate to the type of service (such as storage, processing, bandwidth, and active user accounts).

CLOUD COMPUTING MODELS



IT OUTSOURCING

- IT service outsourcing is the practice of hiring another company to perform some or all of your IT operations functions (that is, hiring the company to provide the people and processes necessary to perform the function).
  - **Onsite -** This model is used when a company outsources an operation but wants or needs for that function to be performed on company property.
  - **Offsite -** This model is used when a company outsources an operation without any onsite activity. Not only is the external company responsible for providing the personnel and processes necessary for performing the function, but they are also responsible for providing the facilities and infrastructure necessary for performing the function (often with connectivity back to the hiring company).

AUDITING CLOUD ENVIRONMENTS

- This gets a little more involved as you have to audit both the client, and the third-party cloud provider.
- **A lot of clients think that their cloud environments don't need to be audited because they're "secure" since they're "on the cloud".**
  - **Wrong…**
- Third party reports and certifications make things a little easier.

THIRD-PARTY REPORTS AND CERTIFICATIONS

- Statements on Standards for Attestation Engagements No. 18, or SSAE 18
- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27000 series, including ISO/IEC 27001, ISO/IEC 27002, and ISO/IEC 27018
- Health Information Trust Alliance (HITRUST)
- Cloud Security Alliance Security Trust Assurance and Risk (STAR)
- Federal Risk and Authorization Management Program (FedRAMP)

SPECIAL NOTE ON CLOUD AUDITING

- An additional risk of outsourcing to the cloud is that you're not in total control of your data or your environment anymore.
- Who at the cloud vendor has access to your data?
- Very important audit point: "Determine how vendor employees access your systems and how data is controlled and limited."