WILMINGTON
UNIVERSITY

Agenda

- Introduction
- Trends
- Cloud Background
- Cloud Security
- Cloud Threats
- Key Takeaways

WILMINGTON UNIVERSITY®

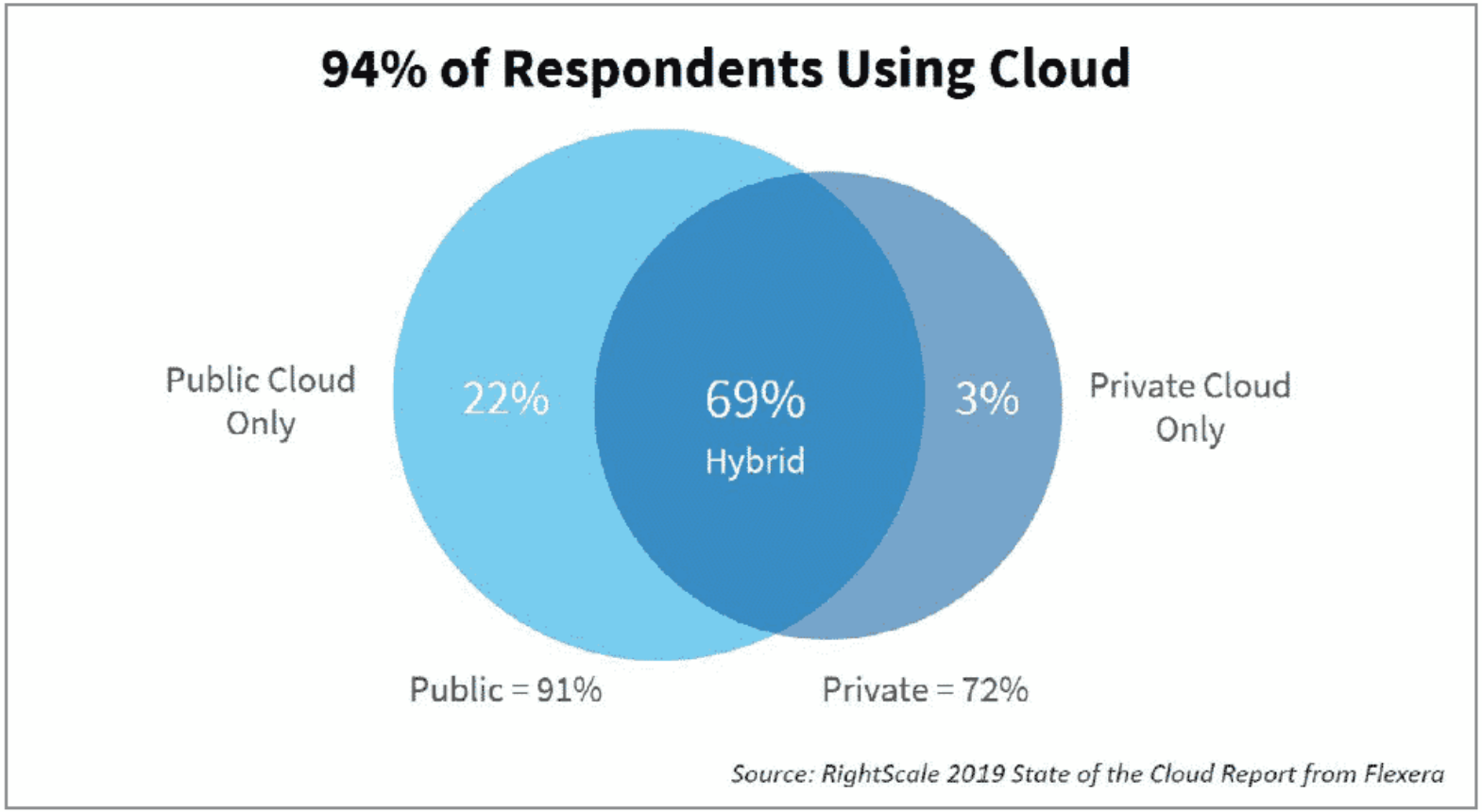
INTRODUCTION

Introduction

TRENDS

WILMINGTON UNIVERSITY®

Cloud Trends

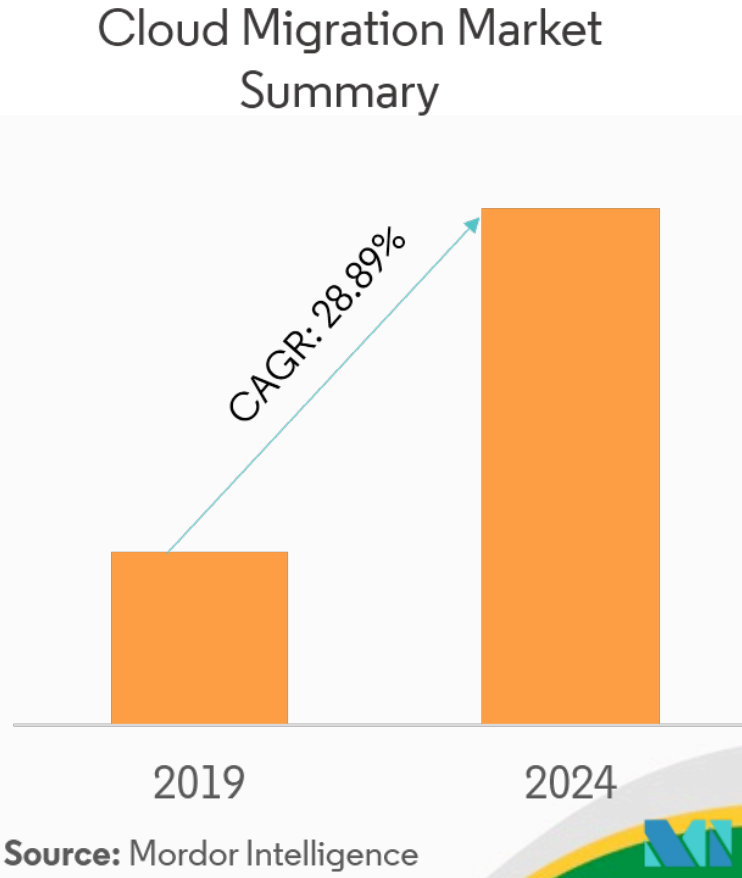


Why talk about Cloud Security?

Market Size: $411B by 2020 (CenturyLink)

Growth 28.89% CAGR (Modor)

Businesses & Customers use over
100 distinct cloud services TODAY! (Contegix LLC)



Threat Landscape

Top Threats 2017	Assessed Trends 2017	Top Threats 2018	Assessed Trends 2018	Change in ranking
1. Malware	Stable	1. Malware	Stable	→
2. Web Based Attacks	Increasing	2. Web Based Attacks	Increasing	→
3. Web Application Attacks	Increasing	3. Web Application Attacks	Stable	→
4. Phishing	Increasing	4. Phishing	Increasing	→
5. Spam	Increasing	5. Denial of Service	Increasing	↑
6. Denial of Service	Increasing	6. Spam	Stable	↓
7. Ransomware	Increasing	7. Botnets	Increasing	↑
8. Botnets	Increasing	8. Data Breaches	Increasing	↑
9. Insider threat	Stable	9. Insider Threat	Declining	→
10. Physical manipulation/ damage/ theft/loss	Stable	10. Physical manipulation/ damage/ theft/loss	Stable	→
11. Data Breaches	Increasing	11. Information Leakage	Increasing	↑
12. Identity Theft	Increasing	12. Identity Theft	Increasing	→
13. Information Leakage	Increasing	13. Cryptojacking	Increasing	NEW
14. Exploit Kits	Declining	14. Ransomware	Declining	↓
15. Cyber Espionage	Increasing	15. Cyber Espionage	Declining	→

Legend: Trends: Declining, Stable, Increasing
Ranking: ↑Going up, → Same, ↓ Going down

Table 1- Overview and comparison of the current threat landscape 2018 with the one of 2017

WILMINGTON UNIVERSITY®

CLOUD BACKGROUND

Cloud Defined

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Citation: Special Publication (NIST SP) - 800-145

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

WILMINGTON UNIVERSITY®

Cloud Basics

- Features
  - Services - Use of internet-based services to support business process
  - Rent IT-services on a utility-like basis
- Key Attributes
  - Rapid deployment
  - Low startup costs/ capital investments
  - Costs based on usage or subscription
  - Multi-tenant sharing of services/ resources
- Essential characteristics
  - On demand self-service
  - Ubiquitous network access
  - Location independent resource pooling
  - Rapid elasticity
  - Measured service

"Cloud computing is a compilation of existing techniques and technologies, packaged within a new infrastructure paradigm that offers improved scalability, elasticity, business agility, faster startup time, reduced management costs, and just-in-time availability of resources" NIST

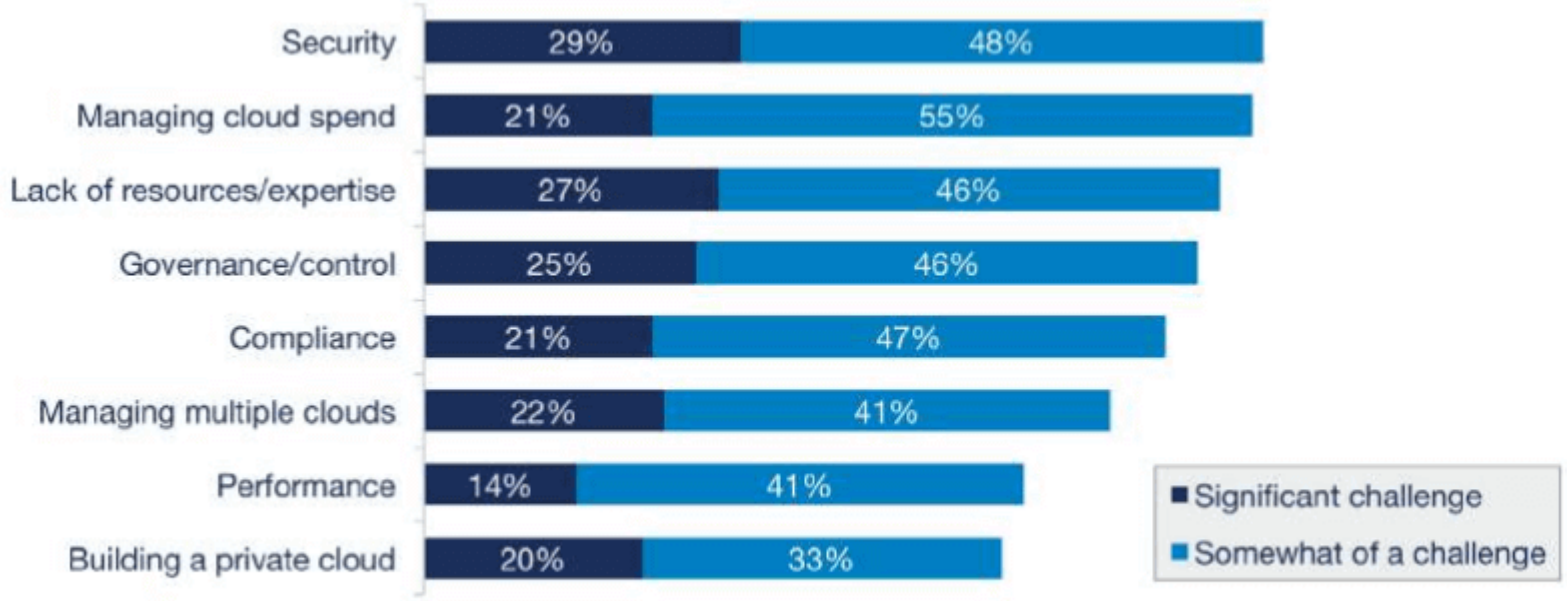
WILMINGTON UNIVERSITY®

Why Migrate to a Cloud Strategy?

- Purchasing - Service
  - Efficiency – Save $$ and Time
- Reliability - Availability
- Scalability – Elasticity & Capacity
- Manageability
- Cost effective
- Resourcing (Skillsets/People)

WILMINGTON UNIVERSITY®

Cloud Concerns



Source: RightScale 2018 State of the Cloud Report

WILMINGTON UNIVERSITY®

Resistance to Cloud Adoption

- Security
- Operational Control
- Service Level Agreements –
  Cloud Service Provider (CSP)
- Governance
- Regulatory Issues (Documentation)

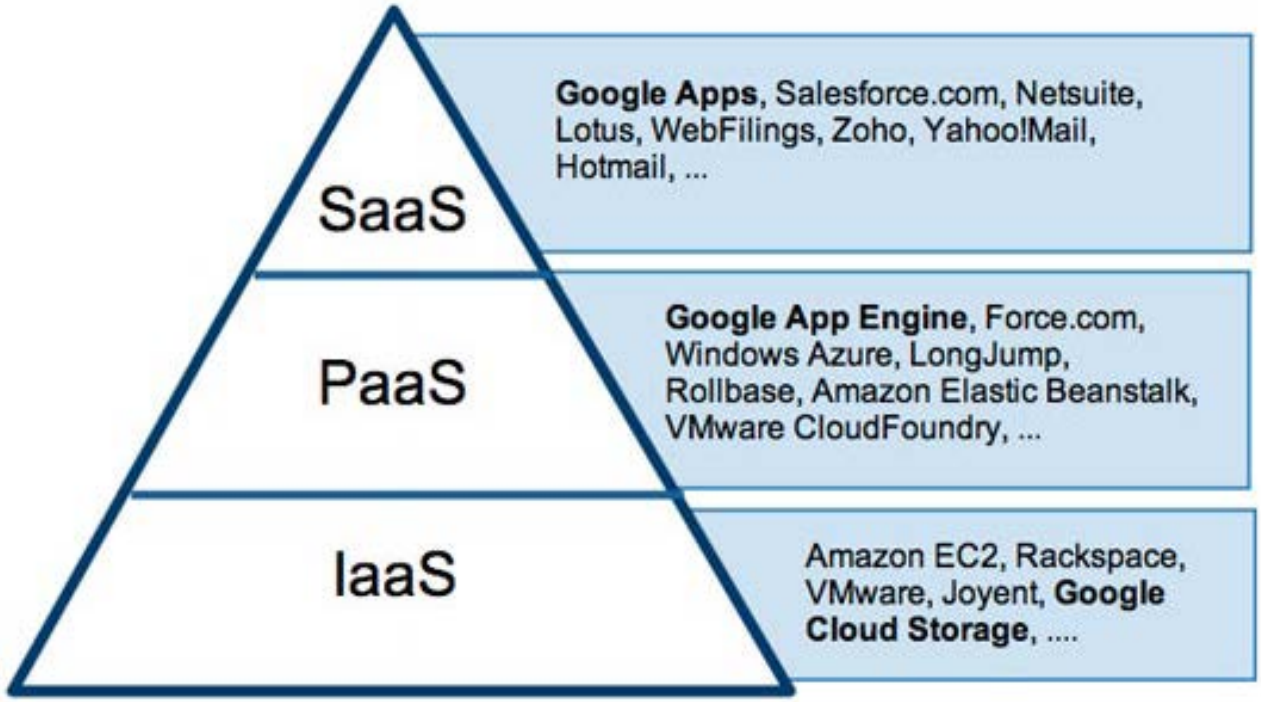
WILMINGTON UNIVERSITY®

Cloud Service Models

- Infrastructure as a Service (IaaS)
  - Standardized, highly automated offering, where compute resources, complemented by storage and networking capabilities are owned by a service provider and offered to customers on-demand. Customers are able to self-provision the infrastructure.
- Platform as a Service (PaaS)
  - Offering is a broad collection of application infrastructure (middleware) services including application platform, integration, business process management and database services.
- Software as a Service (SaaS)
  - Software is owned, delivered and managed remotely by a provider. The provider delivers software based on one set of common code and data definitions that is by contracted customers on a pay-for-use basis or as a subscription.

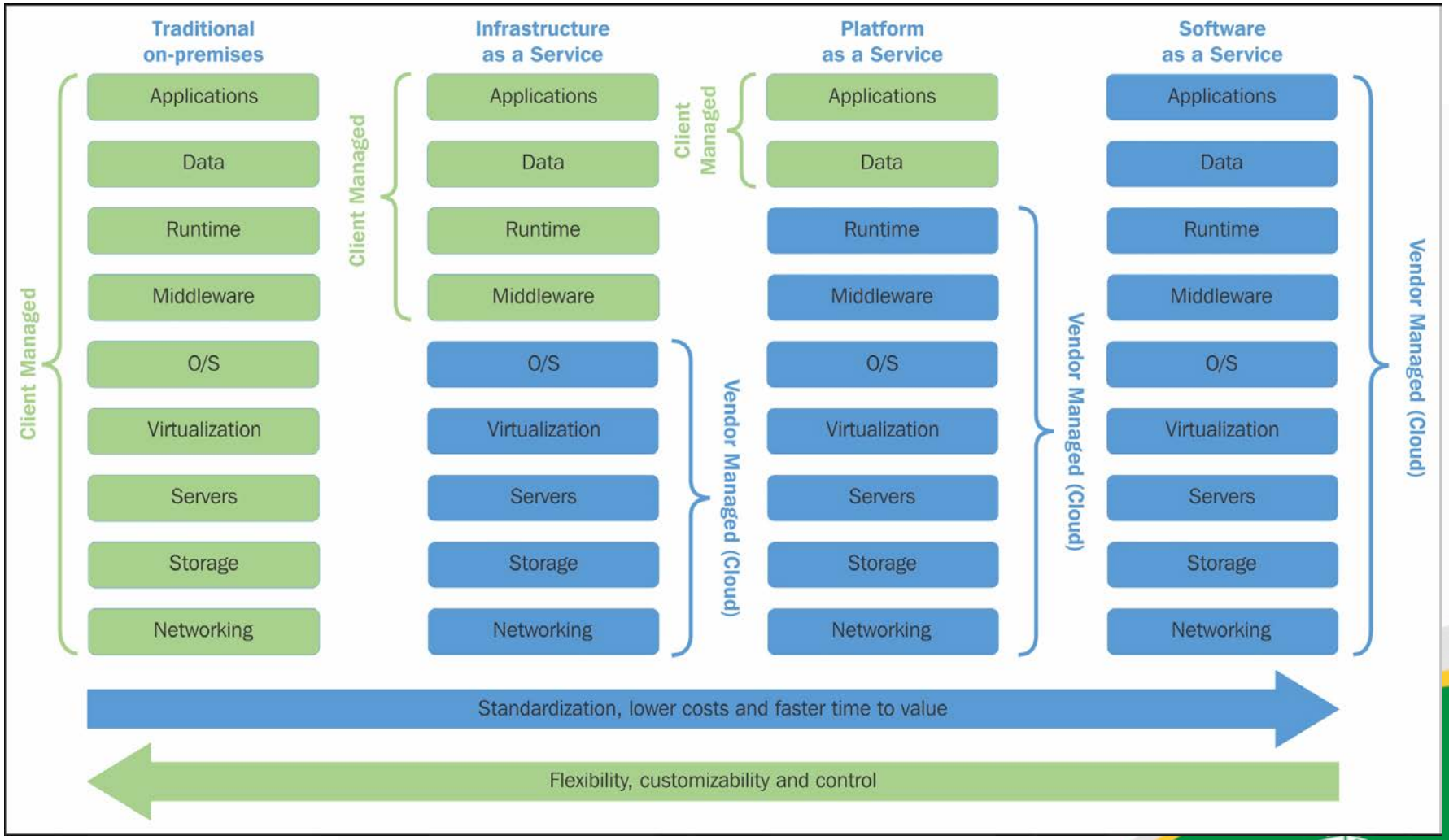
WILMINGTON UNIVERSITY®

Cloud as Gartner Defines It



WILMINGTON UNIVERSITY®

Cloud Service Models



Cloud Deployment Models

	Infrastructure Owned by	Managed by	Where?
Public	CSP	CSP or 3rd Party	CSP Data Center
Private	Organization	Organization	On-premise
Hybrid	Shared	Shared	Depends
Community	Shared	Shared	Depends

WILMINGTON UNIVERSITY®

CLOUD SECURITY

WILMINGTON UNIVERSITY®

Bringing the Pieces Together

Cloud Security

- Outsource On-Premise Security
- Same Security controls – CSP provides
  - Stand alone servers
  - Physical servers in a data center
  - Virtualization in a data center
  - Protect/Encrypt data at rest/transit
- Few differences in terms of what controls – the issue is **who**
- Organizations feel vulnerability as they lose control
- Organizations need to document and detail controls

WILMINGTON UNIVERSITY®

Cloud Security Advantages

- Unified Platform Environment – limited set of variables
- Uniform environment – best practice
- Regulate Access to Compute and Storage Resources
- Certified technical specialists and resources
- Backup, Recovery and Incident Processes
- Data concentration for mobile users

WILMINGTON UNIVERSITY®

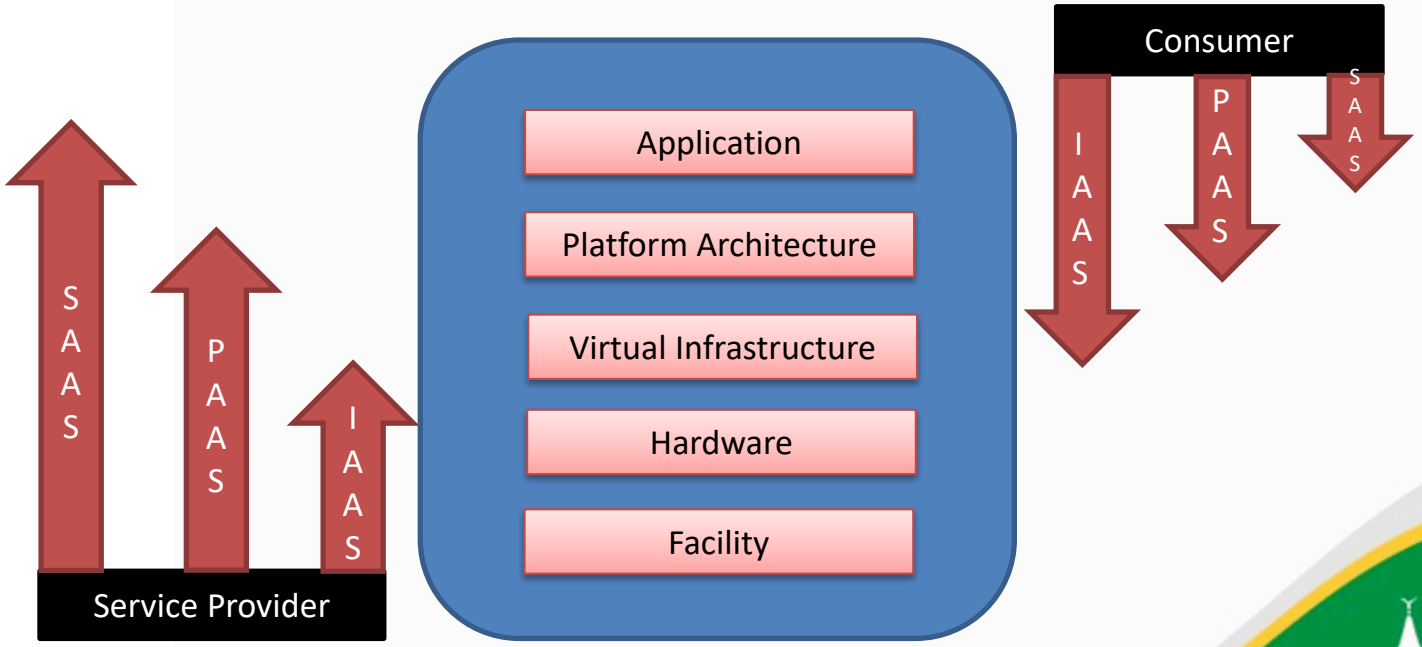
Cloud Security Disadvantages

- Downtime/Outages – Failover DR/BC
- Security and Privacy – Reliant on 3rd Party
- Centralized Attack Profile – Compute, Storage, and Data
- Limited Control and Flexibility – Provisioning
- Vendor Security Model
- Access
- Multi-tenant

WILMINGTON UNIVERSITY®

Shared Security Model

- In terms of security – the CSP and Consumer roles are related to cloud service model – but they are inverse to each other.



NIST SP 800-53

- AC - Access Control
- AU - Audit and Accountability
- AT - Awareness and Training
- CM - Configuration Management
- CP - Contingency Planning
- IA - Identification and Authentication
- IR - Incident Response
- MA – Maintenance
- MP - Media Protection
- PS - Personnel Security
- PE - Physical and Environmental Protection
- PL - Planning
- PM - Program Management
- RA - Risk Assessment
- CA - Security Assessment and Authorization
- SC - System and Communications Protection
- SI - System and Information Integrity
- SA - System and Services Acquisition

WILMINGTON UNIVERSITY®

Architectural Considerations

- Attack Surface.
  - The hypervisor is an additional layer of software between an operating system and hardware platform. The hypervisor normally supports other application programming interfaces to conduct administrative operations, such as launching, migrating, and terminating virtual machine instances. This increases the attack surface.

- Complicated Architectures
  - Virtual machines environments and their supportive software are complicated. Implementing organizational software in PaaS or IaaS creates additional complications that have to managed appropriately

WILMINGTON UNIVERSITY®

Architectural Considerations

- Virtual Network Protection
  - Most virtualization platforms have the ability to create software-based switches and network configurations as part of the virtual environment to allow virtual machines on the same host to communicate more directly and efficiently. Some hypervisors' network monitoring capabilities are not as robust as physical network tools.
- Virtual Machine Images.
  - IaaS cloud providers maintain repositories of virtual machine images. A virtual machine image includes a the software stack and speeds up the time to implementation. These are often shared. Shared virtual images must be validated and carefully controlled to not implement problems.

WILMINGTON UNIVERSITY®

Architectural Considerations

- Client-Side Protection
  - Web browsers, a key element for many cloud computing services, and the various plug-ins and extensions are notorious for their security problems. Security awareness is as important when dealing with a cloud application as any other alternately implemented application.
- Identify and Access Management
  - Identification, authentication, authorization and accounting are critical to implement, enforce and monitor on any cloud based applications or cloud management portals.

WILMINGTON UNIVERSITY®

Cloud Governance

- Cloud Governance by the Customer is Critical
  - Cloud Customers need to define cloud strategy before entering into agreement with CSP
  - Organizational assets agreed upon and assessed for suitability for cloud
  - Partner with business units or functions
  - Outline phased approach to cloud journey
  - Document issues, exceptions, restrictions, and risks
  - Document regulatory and compliance requirements
  - Document business and system interdependencies.

WILMINGTON UNIVERSITY®

Cloud Governance

- Cloud Governance by the Customer is Critical
  - Evaluate organizational practices, policies, procedures, and standards for implementation
  - Review policies, procedures and standards implemented for application development and service provisioning.
  - Establish/Reinforce standards and procedures with development, testing (application and data), staging, training, production and disaster recovery in alignment with organizational policies, guidelines, and standards.
  - Develop audit mechanisms and tools to ensure organizational practices are being followed and ensure proper measures are in place to remediate non-compliance

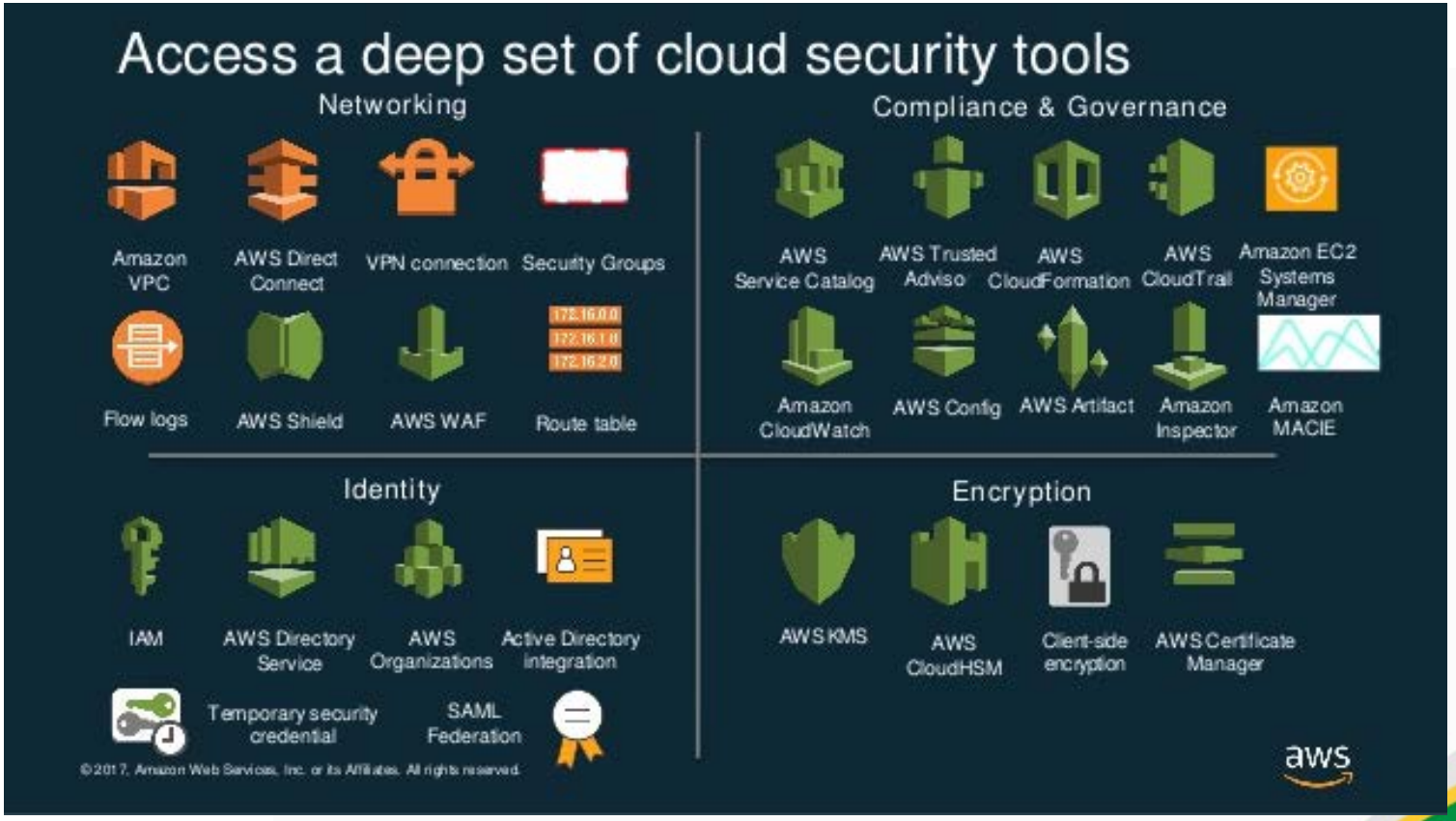
WILMINGTON UNIVERSITY®

Cloud Operations & Maintenance

- Fault management
- Problem management
- Equipment management
- Change management
- Release management
- Supplier management
- Prevention management
- Resource staffing
- Architectural/network topology documentation

WILMINGTON UNIVERSITY®

Cloud Compliance



Availability

Primary Risks to System Availability

According the survey respondents, the top five risks to system availability are:

1. Application bugs
2. Network failures
3. Human errors
4. Cloud provider downtime
5. Application scalability limitations

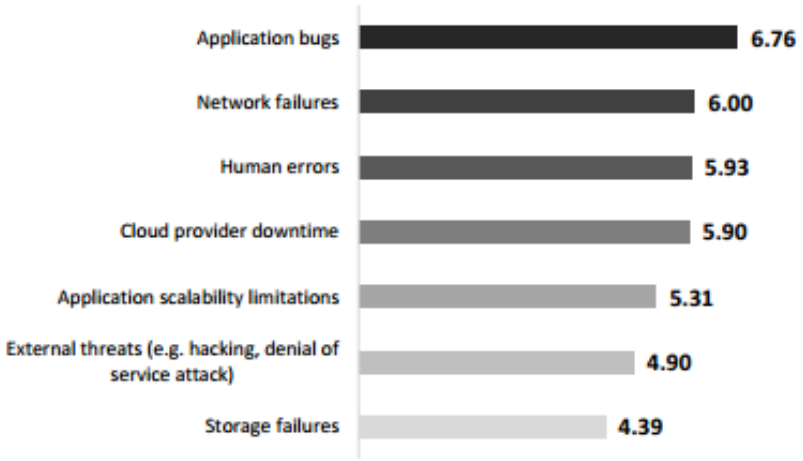


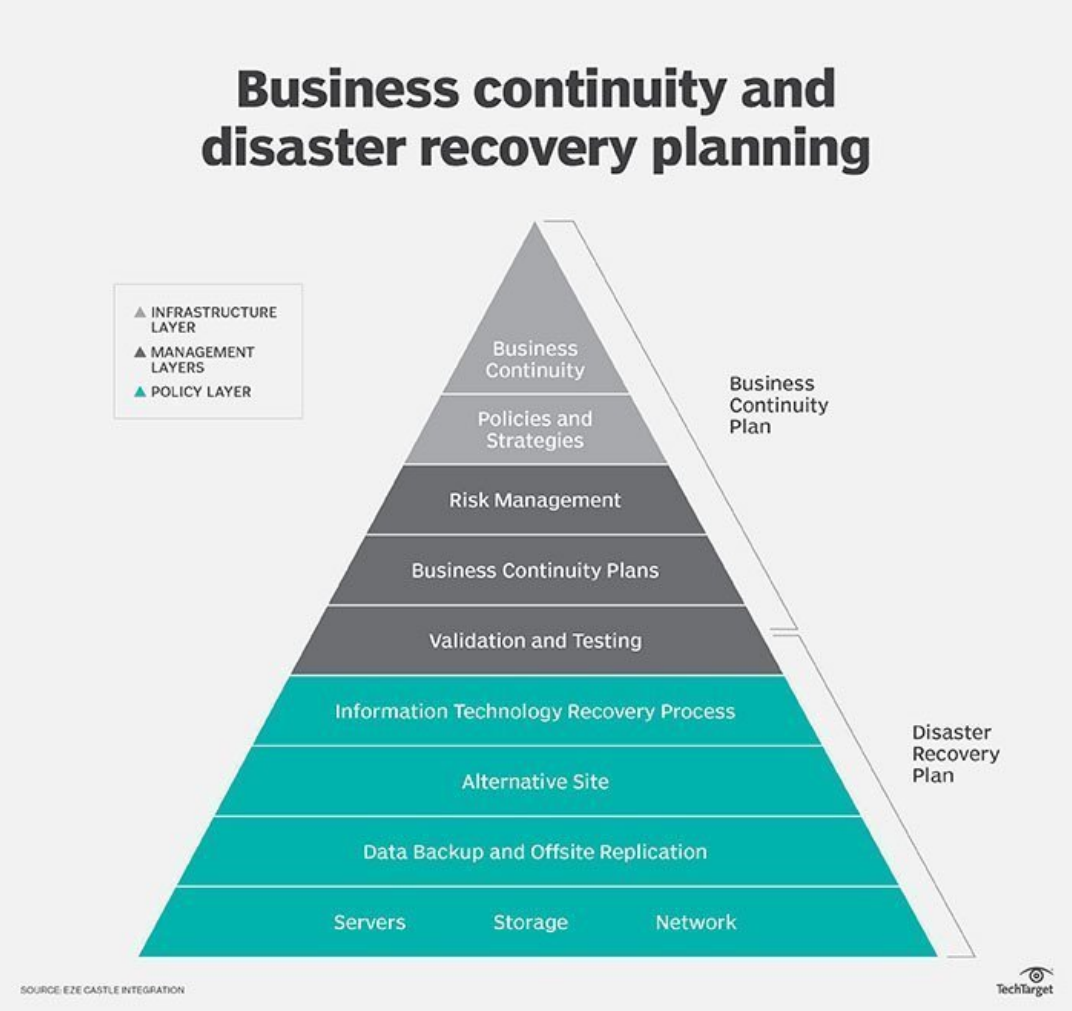
Figure 15: Primary risks to system availability (1-10 scale)

Availability - Regions

Cloud Regions	AWS	Azure	Google
US	4	8	4
Americas	2	3	2
Europe	4	8	5
Asia Pacific	8	13	5

WILMINGTON UNIVERSITY®

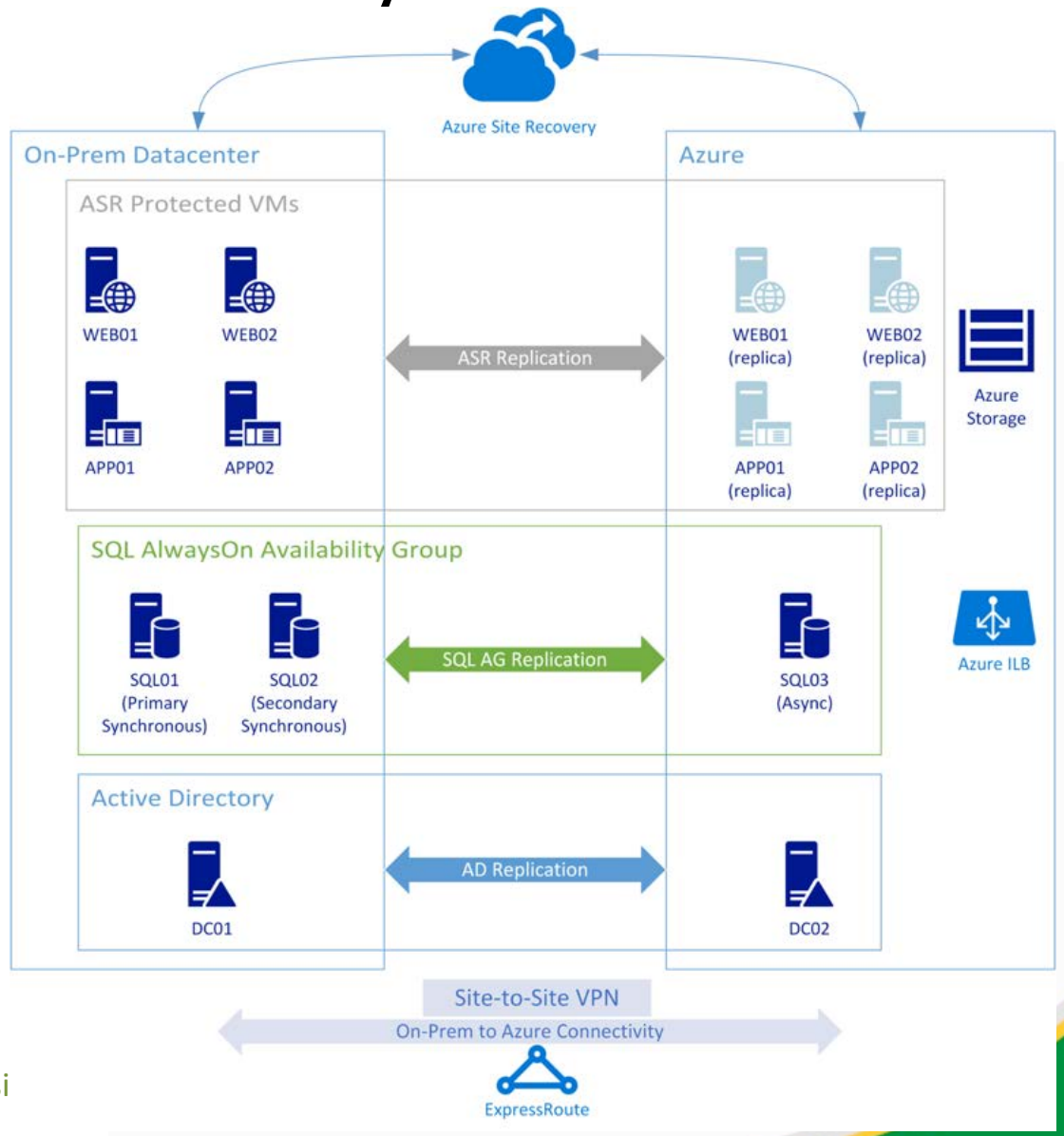
Disaster Recovery and Business Continuity



Disaster Recovery and Business Continuity

- Server Images (Base+)
- Systems
- Applications
- Data and Databases
- Access Control Information
- Workstations (CLI)

Disaster Recovery and Business Continuity



WILMINGTON UNIVERSITY®

Identity and Access Management

- Identity Management includes:
  - Self-service
  - Registration
  - Password management
  - Provisioning
- Access Management includes:
  - Authentication
  - Authorization
  - Policy Management
  - Federation
  - Identity Repository

WILMINGTON UNIVERSITY®

Identity and Access Management

- Identity repositories provide directory services for the administration of user accounts and their attributes.
- Common Directory Services:
  - X.500 and LDAP
  - Microsoft Active Directory
  - Metadata replication and synchronization
  - Directory as a Service

WILMINGTON UNIVERSITY®

CLOUD THREATS

WILMINGTON UNIVERSITY®

Cloud Threats

Threats

- Malicious Code
  - Ransomware
  - Virus
  - Worms
  - Trojans
  - Logic bombs
  - Malware
  - Botnet
- Malicious Code Countermeasures
  - Scanners
  - IDS/IPS
  - Security testing
  - Anti-malware
  - Code signing
  - Sandboxing
  - Appropriate patching

WILMINGTON UNIVERSITY®

Threats

- Malicious Activity
  - Social Engineering
  - Privilege Escalation
  - Spoofing
  - Phishing
  - Spam
  - Botnets
- Malicious Activity Countermeasures
  - Controlled and Managed User Access
  - Limit and Segment Developer/Admin Privileges
  - System Hardening
  - Patching
  - Staging - Test/Dev/Production Environments
  - Policies and Procedures

WILMINGTON UNIVERSITY®

Threats

- Abuse and Nefarious use
  - Hackers continue to leverage technologies to improve their reach, avoid detection, and improve the effectiveness of their activities.
  - Cloud providers are actively being targeted, partially because their relatively weak registration systems facilitate anonymity, and providers' fraud detection capabilities are limited
- Countermeasures: Patching, intrusion detection, security awareness training, background checks

WILMINGTON UNIVERSITY®

Threats

- Insecure interfaces and APIs
  - Cloud providers strive to provide security and that it is integrated into their service models.
  - Consumers of services need to understand the security implications associated with the usage, management, orchestration and monitoring of cloud services.
  - Reliance on a weak set of interfaces and APIs exposes organizations to a variety of security issues related to confidentiality, integrity, availability and accountability

- Countermeasures: Architecture review, security testing, patching schedules, Service Level Agreements, legal agreements (BAA)

WILMINGTON UNIVERSITY®

Threats

- Insider Threat
  - The impact that malicious insiders can have on an organization is great because of their level of access and understanding of data and information technology assets.
  - Theft, reputation damage and loss of productivity are some examples of how malicious insider can affect an operation.
  - Organizations that adopt cloud services need to understand the human element and that the responsibility for a malicious insider is relevant for staff of the cloud provider.

- Countermeasures: Background checks, policies and procedures, non-repudiation, two man work, security awareness training, least privilege

WILMINGTON UNIVERSITY®

Threats

- Shared technology issues
  - Attacks have surfaced in recent years that target the shared technology inside cloud computing environments.
  - As a result, attackers focus on how to impact the operations of other cloud customers, and how to gain unauthorized access to data.

- Countermeasures: Patching, security testing, monitoring, security awareness training

WILMINGTON UNIVERSITY®

Threats

- Data loss or leakage
  - Data loss or leakage can have a devastating impact on a business and its impact is directly relevant to the type of data.
  - Compliance violations, legal ramifications
  - Loss of core intellectual property could have competitive and financial implications

- Countermeasures: Data Loss Prevention Applications, encryption, security awareness training, data classification, policies and procedures, least privilege

WILMINGTON UNIVERSITY®

Threats

- Account or service hijacking
  - Account and service hijacking, usually with stolen credentials, remains a top threat. With stolen credentials, attackers can often access critical cloud services, allowing them to compromise the confidentiality, integrity and availability of the services and the data

- Countermeasures: Policies and procedures, security awareness training, enforced password life, complexity and reuse

WILMINGTON UNIVERSITY®

Threats

- Unknown Risk Profile
  - When adopting a cloud service, the features and functionality may be well advertised, but organizations need to understand the cloud service security posture/risk/threat profile.
  - Understand the controls or compliance alignment
  - Ensure the CSP has the necessary internal security procedures, configuration hardening, patching, auditing, and logging
  - Understand and verify the audits and certifications of the CSP
  - Be explicit regarding accessing and extracting various systems logs
  - Understand whether you can conduct vulnerability scanning and/or penetration testing
  - Ask if the provider shares vulnerability scanning and testing results
- Countermeasures: Research, agreements, and governance

WILMINGTON UNIVERSITY®

KEY TAKEAWAYS

WILMINGTON UNIVERSITY®

Key Points - Business

- Perform and exercise a due diligence process when selecting a cloud service provider (CSP).
- Ensure you have a realistic monthly/yearly cost/budget
- Establish and understand detailed Service Level Agreements (SLAs) to ensure performance
- Engage Cloud specific legal advice before moving to the cloud.
- Ensure the CSP supports the regulatory requirements of your organization and data.
- Clearly understand the type of cloud service model your need - IaaS, PaaS, SaaS or other model.

WILMINGTON UNIVERSITY®

Key Points - Technical

- Ensure you have a realistic schedule to setup servers (VMs), applications and data center to the cloud.
- Partner with business owners to assess and classify data to understand the sensitivity and risk of your data before moving to the cloud
- Clearly define who owns the data and the retention/disposal requirements associated with data in the event you cancel the contract
- Understand that many organizational policies and procedures will need to be updated and upgraded for cloud.
- When using data provided by 3rd parties note that you may need to notify and append current license and date use agreements

WILMINGTON UNIVERSITY®

QUESTIONS?

WILMINGTON UNIVERSITY®