

REPORT DOCUMENTATION PAGE					Form Approved OMB No. 0704-0188	
<p>The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.</p> <p><b>PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.</b></p>						
1. REPORT DATE (DD-MM-YYYY) 11/05/2020		2. REPORT TYPE Technical Report			3. DATES COVERED (From - To)	
4. TITLE AND SUBTITLE Cloud Computing Technical Exchange				5a. CONTRACT NUMBER W56KGU-18-D-0004		
				5b. GRANT NUMBER		
				5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S) Reavey, Michael				5d. PROJECT NUMBER		
				5e. TASK NUMBER		
				5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) The MITRE Corporation 202 Burlington Road Bedford, MA 01730				8. PERFORMING ORGANIZATION REPORT NUMBER PRS-20-2788		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)		
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)		
12. DISTRIBUTION/AVAILABILITY STATEMENT DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.						
13. SUPPLEMENTARY NOTES						
14. ABSTRACT 1-Definition, 2-Policy and Strategy, 3-Adoption/Migration, 4-Security, 5-Economics, 6-Workforce Development, 7-Cloud DevSecOps, 8-References						
15. SUBJECT TERMS Computing Methodologies (General); Computer Security; Network Security cloud computing; adoption; ATT&CK; federal policy; migration; strategy;						
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES  56	19a. NAME OF RESPONSIBLE PERSON Susan Carpenito	
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER (Include area code) 781-271-7646	

# Cloud Computing Technical Exchange

**Michael Reavey**

**November 05, 2020**

Approved for Public Release  
Distribution Unlimited. Public Release Case Number 20-2788

The views, opinions, and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

This technical data deliverable was developed using contract funds under Basic Contract No. W56KGU-18-D-0004.

**MITRE**

**SOLVING PROBLEMS  
FOR A SAFER WORLD™**

© 2020 THE MITRE CORPORATION.

# **Outline**

**Definition**

**Policy and Strategy**

**Adoption/Migration**

**Security**

**Economics**

**Workforce Development**

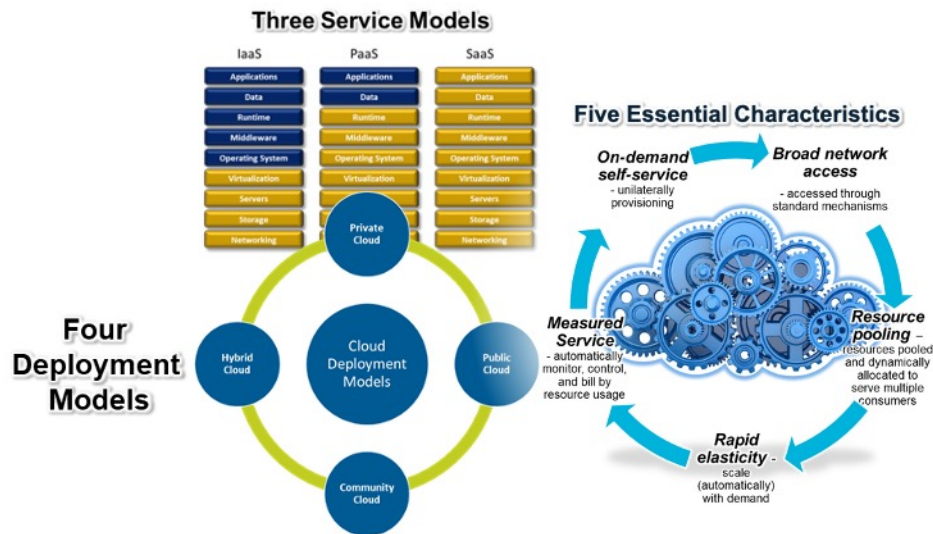
**Cloud DevSecOps**

**References**

**Backup**

# Definition

# NIST Definition of Cloud Computing



MITRE

© 2020 THE MITRE CORPORATION.

4

Slide Source: MITRE

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. [1]

- Pay-per-Use – Pay only for the IT resources you use
- Resource Pooling - Shared, multi-tenant, location-independent
- On-demand - Self-service, real-time, automatic provisioning
- Network Accessible - Available over the Internet
- Elastic - Automatically scaled up and down as needed

## NIST Service Models

Area of Responsibility	NIST Model			Traditional
	SaaS	PaaS	IaaS	On-Premise
Data Governance & Rights	Mission Owner	Mission Owner	Mission Owner	Mission Owner
Client Endpoints	Mission Owner	Mission Owner	Mission Owner	Mission Owner
Account and Access Management	Mission Owner	Mission Owner	Mission Owner	Mission Owner
Identity and Directory Services	Shared	Shared	Mission Owner	Mission Owner
Applications	CSP	Shared	Mission Owner	Mission Owner
Network Security Controls	CSP	Shared	Mission Owner	Mission Owner
Operating System Patches and Versions	CSP	CSP	Mission Owner	Mission Owner
Hosting Infrastructure (Virtualization, Servers, Storage)	CSP	CSP	CSP	Mission Owner
Network Infrastructure	CSP	CSP	CSP	Mission Owner
Physical Data Center	CSP	CSP	CSP	Mission Owner

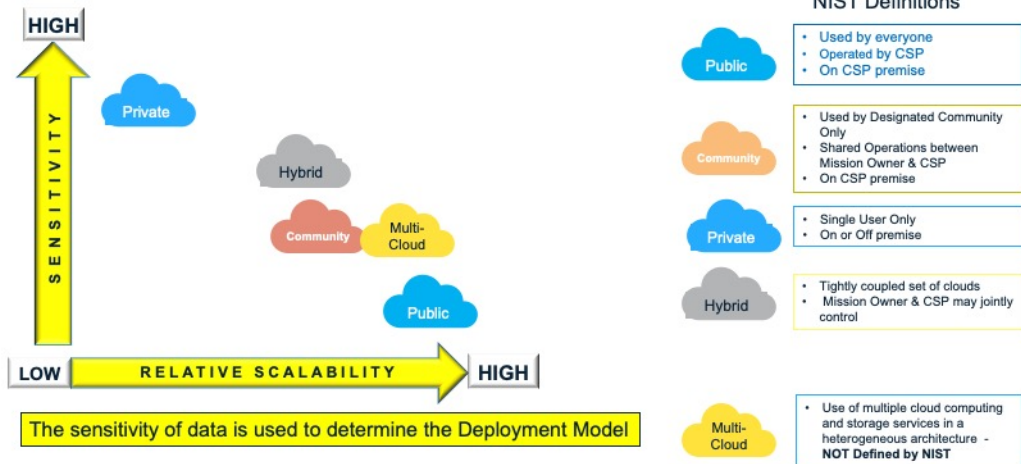
The type of workload is used to determine the Service Model

Always Mission Owner Responsibility

SP 800-145: The NIST Definition of Cloud Computing

Slide Source: MITRE

# NIST Deployment Models



Slide Source: MITRE

# Common Cloud Use Cases



## Establish Pipelines

Development, test, staging, and production environments



## Modernize and Increase Mission Capability

Redeploy legacy systems, leverage newer tech (IoT, AI/ML)



## Expand Capacity

Additional compute, storage and network resources



## Increase Performance

Availability, Scalability, Continuity

Slide Source: MITRE



## Common Cloud Challenges

### Limitations

- Budget
- Workforce
- Asset Visibility

### Concerns

- Loss of Security
- Loss of Control
- Vendor Lock-in

### Uncertainty

- Decision-Making
- Acquisition Strategy

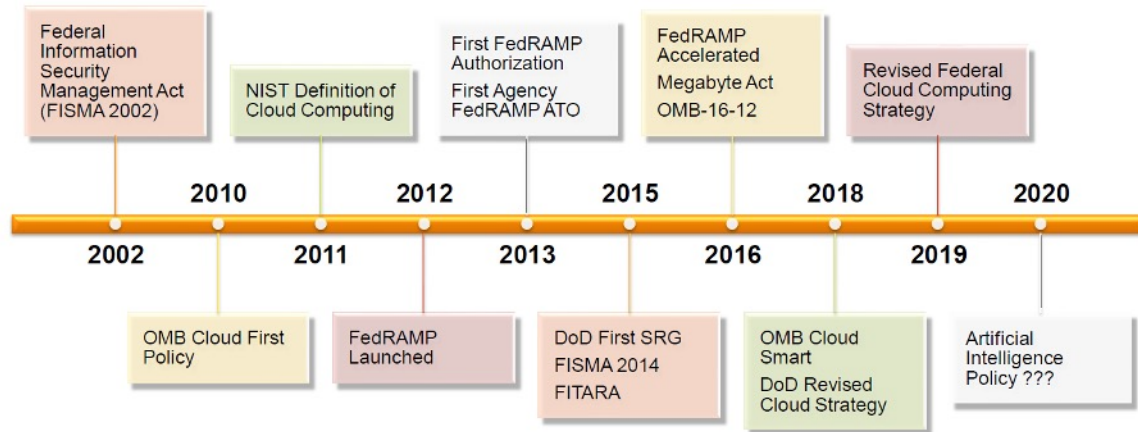
### Complexity

- Systems
- Infrastructures

Slide Source: MITRE

# Policy and Strategy

## Federal Policy & Guidance Timeline



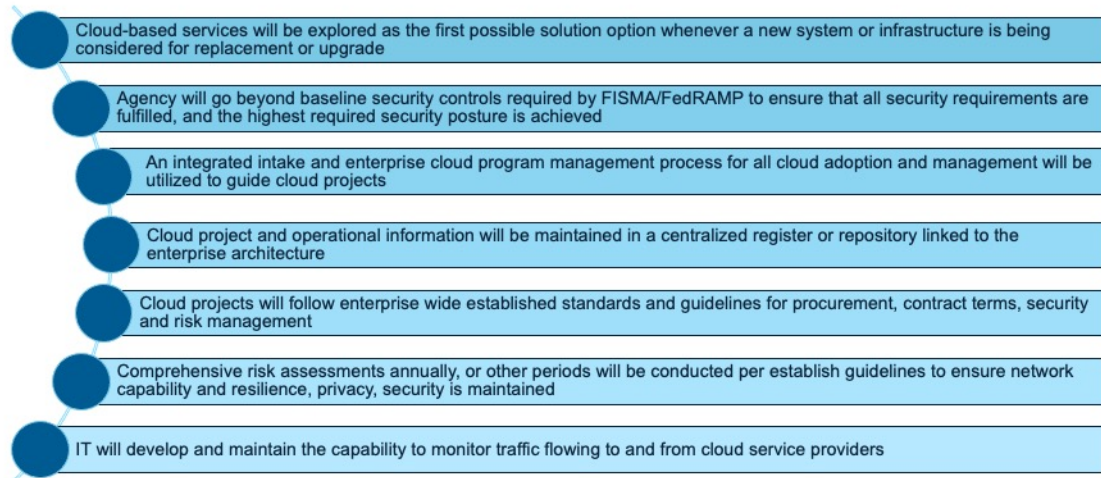
MITRE

© 2020 THE MITRE CORPORATION.

10

Slide Source: MITRE

## Cloud Guiding Principles – Cloud Smart

- 
- Cloud-based services will be explored as the first possible solution option whenever a new system or infrastructure is being considered for replacement or upgrade
  - Agency will go beyond baseline security controls required by FISMA/FedRAMP to ensure that all security requirements are fulfilled, and the highest required security posture is achieved
  - An integrated intake and enterprise cloud program management process for all cloud adoption and management will be utilized to guide cloud projects
  - Cloud project and operational information will be maintained in a centralized register or repository linked to the enterprise architecture
  - Cloud projects will follow enterprise wide established standards and guidelines for procurement, contract terms, security and risk management
  - Comprehensive risk assessments annually, or other periods will be conducted per establish guidelines to ensure network capability and resilience, privacy, security is maintained
  - IT will develop and maintain the capability to monitor traffic flowing to and from cloud service providers

Slide Source: MITRE

Cloud First (2011) evolved to Cloud Smart (2019)

## DoD Policy Requirements



Prescribed by Defense Federal Acquisition Regulation Supplement Subpart 239.76, which states that DOD must generally acquire Cloud services using commercial terms and conditions consistent with federal law and DOD's needs.



A contract to acquire Cloud services may generally only be awarded to a provider (e.g., a prime contractor or subcontractor) with provisional Defense Information Security Agency (DISA) authorization to provide such services, consistent with the current version of the DOD Cloud Computing Security Requirements Guide.



DOD Instruction 5000.74, Defense Acquisition of Services, specifies that all Cloud services must have an Authority to Operate (see also DOD Instruction 8510.01, Risk Management Framework for DOD Information Technology)



DOD Memorandum Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services, issued on December 15, 2014, provides additional guidance for the acquisition of commercial Cloud services

MITRE

© 2020 THE MITRE CORPORATION.

Slide Source: MITRE

Source: Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services (2014) [2]

DoD Cloud Acquisition [Business](#) Requirements:

Analyze Cloud Services using DoD Memorandum, "Use of Enterprise Information Technology Standard Business Case Analysis," October 23, 2014.

DISA provided cloud services must be considered as part of the BCA.

DoD Cloud Acquisition [Security](#) Requirements:

Publicly released, Unclassified DoD information may be hosted on FedRAMP approved cloud services.

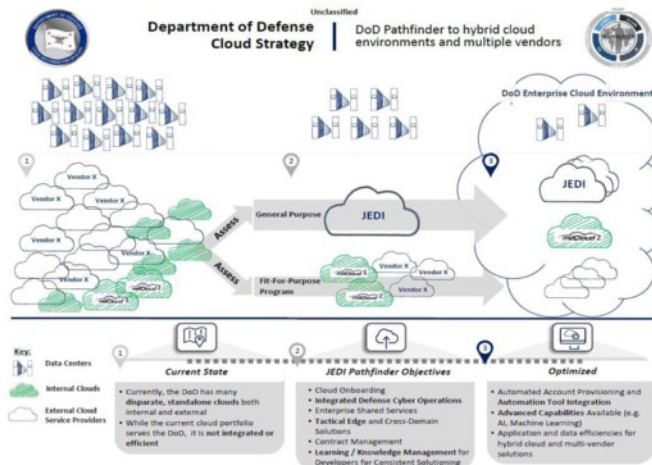
For more sensitive data, cloud providers must consult the DoD Cloud Computing Security Requirements Guide (SRG) and receive a DoD Provisional Authorization (PA).

Commercial cloud services for Sensitive Data must be connected to customers through a Cloud Access Point provided by DISA or through a CAP provided by another DoD Component

Components are responsible for cyberspace defense of all information

and missions hosted in commercial cloud services. Requires collaboration and information sharing among the component, DISA, and the CSP.

# DoD Cloud Strategy



Current DoD Strategy published in December 2018

Introduced concepts General Purpose and Fit-for-Purpose

Strategic Objectives:

- Enable Exponential Growth
- Scale for DoD Mission
- Address Cyber Challenges
- Enable AI and Data Transparency
- Extend Tactical Support for Warfighter at the Edge
- Take Advantage of Resiliency in the Cloud
- Drive IT Reform at DoD

MITRE

© 2020 THE MITRE CORPORATION.

13

Slide Source: DoD Cloud Strategy [3]

Note: Current status of protests with JEDI and DEOS are slowly getting resolved, however, effective implementation is still somewhat uncertain

Fit-for-Purpose – when General Purpose cloud can not support mission. Requires approval from the DoD CIO. Should be developed to support the enterprise

# Adoption/Migration



# Cloud Engineering Decision Blueprint

## Pre-Migration Decisions

Application Assessment	CSP Selection	Migration Methods	Cost Estimation	Contract Selection	Workforce Responsibility
Which applications to migrate?	Which offerings to choose?	Which method is most appropriate?	What are the costs and fund types?	Which contracts or agreements?	Who's responsible for what activities?

## Migration Decisions

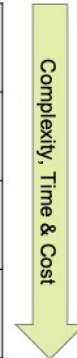
Reference Architectures	Service Offerings	Best Practices	App & Data Protection	Performance Levels	Cost Model
<ul style="list-style-type: none"> <li>What architectures are applicable?</li> <li>What deployments are applicable?</li> </ul>	<ul style="list-style-type: none"> <li>What categories are needed?</li> <li>What offerings are needed?</li> </ul>	<ul style="list-style-type: none"> <li>Which design practices apply?</li> <li>Which security practices apply?</li> </ul>	<ul style="list-style-type: none"> <li>How to secure the environment?</li> <li>How to secure the apps / data?</li> </ul>	<ul style="list-style-type: none"> <li>What performance levels are needed?</li> <li>What SLAs should be written?</li> </ul>	<ul style="list-style-type: none"> <li>How to minimize cost?</li> <li>How to track usage and cost?</li> </ul>

Key decisions that drive cloud adoption

Slide Source: MITRE

## Application Migration Options

<b>Replace</b>	<b>"Drop &amp; Shop"</b>	<ul style="list-style-type: none"> <li>• Replace with SaaS offering</li> <li>• Ideally from CSP's Marketplace</li> </ul>
<b>Rehost</b>	<b>"Lift &amp; Shift"</b>	<ul style="list-style-type: none"> <li>• Move as is, no code change</li> <li>• No benefit from cloud features<sup>1</sup></li> </ul>
<b>Re-Platform</b>	<b>"Rack &amp; Stack"</b>	<ul style="list-style-type: none"> <li>• No code changes</li> <li>• Change platform<sup>2</sup></li> </ul>
<b>Re-Architect</b>	<b>"Shake &amp; Make"</b>	<ul style="list-style-type: none"> <li>• Optimize for cloud</li> <li>• Adopt architectures &amp; best practices</li> </ul>



Note 1. Features: e.g., Auto Scale, Auto Load Balance

Note 2. Platform: OS (e.g., Solaris to Linux), Language (e.g., FORTRAN to Java), Stack (e.g., LAMP to MEAN)  
(LAMP: Linux, Apache, MySQL, PHP) to (MEAN: MongoDB, Express.js, AngularJS, Node.js)

Slide Source: MITRE

## DISA Cloud Adoption Cycle

	LEARN	CHOOSE	BUY	CONFIGURE	TRANSITION	UTILIZE
CLOUD CONSUMER What Mission Partners Should Know and Do...	<ul style="list-style-type: none"> <li>Cloud Policies</li> <li>Goals (Fit, Leverage, Evolve)</li> <li>Information Impact Level</li> <li>Cloud Models</li> <li>Adoption Expertise</li> <li>Outreach</li> </ul>	<ul style="list-style-type: none"> <li>Business/Case Analysis (BCA)</li> <li>Requirement Definition</li> <li>Application Rationalization</li> </ul>	<ul style="list-style-type: none"> <li>Contract Options</li> <li>Period of Performance</li> <li>Color of Money</li> <li>SLA</li> <li>CSSP Services</li> </ul>	<ul style="list-style-type: none"> <li>Specifications</li> <li>Environment</li> <li>Technology</li> <li>Virtual Machine Information</li> </ul>	<ul style="list-style-type: none"> <li>Development/Test</li> <li>User Roles</li> <li>Authentication/Access</li> </ul>	<ul style="list-style-type: none"> <li>Monitor Data Consumption</li> <li>Leverage Cloud Functions</li> <li>Recognize efficiencies</li> </ul>
CLOUD PROVIDER What Cloud Providers Should Tell You...	<ul style="list-style-type: none"> <li>FedRAMP/JAB PA Status</li> <li>Cloud Service Offering</li> </ul>	<ul style="list-style-type: none"> <li>Cost Models</li> <li>Service Models</li> <li>Attributes</li> <li>Service Level Agreement</li> <li>COOP/DR Model</li> </ul>	<ul style="list-style-type: none"> <li>Contract Vehicle</li> <li>On boarding process</li> <li>Consumption visibility</li> </ul>	<ul style="list-style-type: none"> <li>Engineer Support</li> </ul>	<ul style="list-style-type: none"> <li>IA Compliance</li> <li>Transition Support</li> </ul>	<ul style="list-style-type: none"> <li>Operational Transparency</li> <li>Scalability/Flexibility</li> <li>Innovation</li> </ul>

DOES IT MEET THE ORIGINAL NEED?



Slide Source: DISA-Cloud-Playbook-v2.pdf [4]

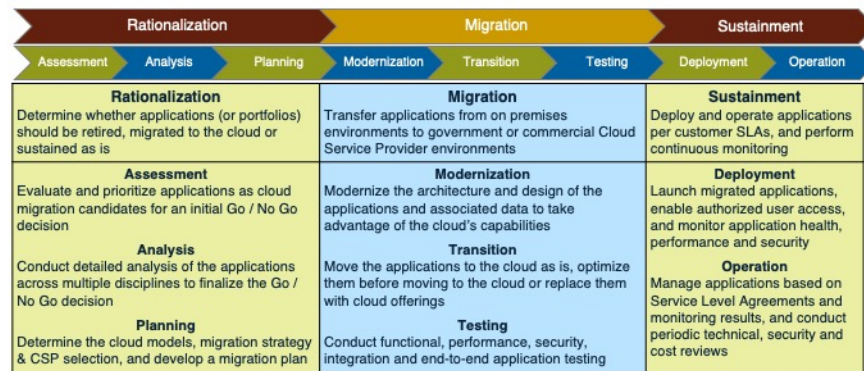
## MITRE Enterprise Cloud Adoption Framework (ECAF)

	Create the Vision	Determine LRP, ROI & Objectives	Establish Governance & EA	Specify Reference Concept	Create Strategy	Develop Measures	Assess IT Investments	Identify Candidates	Implement Cloud	Cloud Operations	Optimize
Political	Use Drivers to Develop Vision, Goals & Priorities	Address Law, Regulation & Policy (LRP) Develop Objectives	Establish Governance and Oversight	Identify Strategic Partnerships	Establish Technology Investment Strategy	Establish Measures Program	Review IT Investment Business Cases	Approve & Fund Best Candidates	Continuously Assess Success	Strategic Partnerships	Continuous Governance & Investment Improvement
Organizational	Develop Use Cases	Identify Stakeholder Objectives	Engage Stakeholders	Identify Process, Organization & Personnel (POP) Impacts	Address Measures Update Acq. Policy	Develop Measures of Capabilities, Costs & Progress	Triage Mission & Business Processes	Update Processes Plan Training	Measure Benefits & Progress	Simplify Processes & Reduce Redundancy	Mature CSP Oversight & Partnership
Economic	Identify Stakeholders	Build Support	Determine Cloud ROI	Understand Cloud Cost Model	Cost Recovery Strategy	Build Cost Measures	Reduce Redundancies Know the CSP Alternatives	Develop Candidate ROIs	Acquire Services	Manage Contracts	Optimize Value
Technological	Establish Risk Tolerance	Analyze State of Technology Applied to Objectives	Establish Technical Enterprise Architecture	Develop Technical Reference Concept	Develop As-Is to To-Be Transition	Establish Technical Measures	Triage IT Systems	Develop Business Cases Determine Migration Type, Architecture	Manage Acq. Risks Develop Migration Plan	Manage Cost Allocation System Development	Maximize Capability
Security	Know Threat Environment	Know Threat Environment	Perform Risk Analysis	Know Vendor Security & Privacy Capabilities	Update Security Policy	Develop Security & Privacy Measures	Consolidate IT Analyze IT Risks	Perform Risk Management Portfolio Analysis	Design System	Deployment A&A	Execute Continuous Monitoring & Security Operations
	Establish Security Tolerance	Know RMF and FedRAMP	Categorize and Select Controls	Define Cloud Security Arch.	Define Cloud Security Arch.	Assess Security & Privacy	Assess Security & Privacy	Assess Security & Privacy	Manage Migration Security Risks	Manage Security & Privacy Threats	

Slide Source: MITRE

Creating Vision, Goals & Priorities is key to adoption success & should be done first  
 ECAF can be used as an assessment tool to determine areas of strengths & weaknesses  
 Identifies interactions & inter-dependence of activities to successfully adopt cloud  
 Flexible & iterative, activities may be revisited as necessary  
 Not a schedule, some activities may be quick, other may be projects  
 Not all areas of the framework may be necessary for every sponsor or situation  
 Some activities may already be cloud ready  
 Not performing an activity potentially increases risks

# MITRE Cloud Engineering Life Cycle









The Cloud Engineering Life Cycle is a structured, iterative and repeatable methodology for developing and migrating applications to the cloud

# AWS Cloud Adoption Framework

The AWS Cloud Adoption Framework (AWS CAF) organizes guidance into six areas of focus, called perspectives.

Each perspective covers distinct responsibilities owned or managed by functionally related stakeholders.

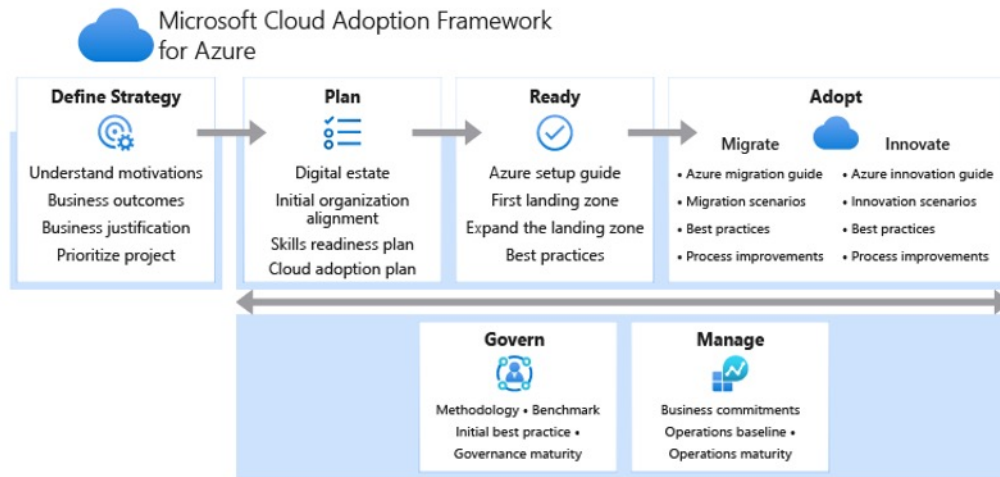
In general, the Business, People, and Governance Perspectives focus on business capabilities; while the Platform, Security, and Operations Perspectives focus on technical capabilities.

<u>Business Capabilities</u>	<u>Technical Capabilities</u>
 BUSINESS	 PLATFORM
 PEOPLE	 SECURITY
 GOVERNANCE	 OPERATIONS

Slide Source:

[https://d1.awsstatic.com/whitepapers/aws\\_cloud\\_adoption\\_framework.pdf](https://d1.awsstatic.com/whitepapers/aws_cloud_adoption_framework.pdf) [5]

# Microsoft Cloud Adoption Framework for Azure



MITRE

© 2020 THE MITRE CORPORATION.

21

Slide Source: <https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/overview> [6]

# Security



# Federal Risk and Authorization Management Program (FedRAMP)

## **FedRAMP is a Government-wide Cloud Program**

Provides standardized approach to security assessment and authorization

Ensures POA&M remediation and continuous monitoring

## **Memo issued by 2<sup>nd</sup> CIO of the US, Steven VanRoekel**

Published to federal agency CIOs on December 8, 2011

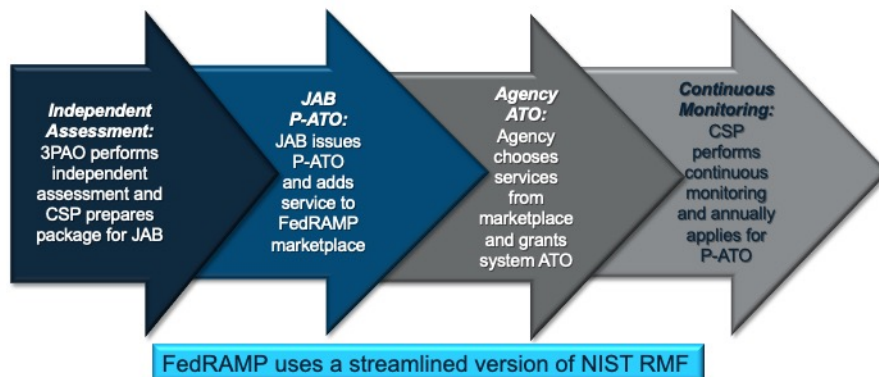
Defining how federal agencies should use FedRAMP

## **Hosted by the Office of Management and Budget (OMB)**



Slide Source: MITRE

## Overall FedRAMP Process



Slide Source: MITRE

3PAO: Third-party assessment organization

P-ATO: Provisional Authority to Operate

JAB: (FedRAMP) Joint Assessment Board

## DoD FedRAMP+ Information Impact Level Comparison

IMPACT LEVEL	INFORMATION SENSITIVITY	SECURITY CONTROLS	LOCATION	OFF-PREMISES CONNECTIVITY	SEPARATION	PERSONNEL REQUIREMENTS
2	PUBLIC or Non-critical Mission Information	FedRAMP v2 Moderate	US / US outlying areas or DoD on-premises	Internet	Virtual / Logical PUBLIC COMMUNITY	National Agency Check and Inquiries (NACI)
4	CUI or Non-CUI Non-Critical Mission Information Non-National Security Systems	Level 2 + CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical Limited "Public" Community Strong Virtual Separation Between Tenant Systems & Information	US Persons ADP-1 Single Scope Background Investigation (SSBI)
5	Higher Sensitivity CUI Mission Critical Information National Security Systems	Level 4 + NSS & CUI-Specific Tailored Set	US / US outlying areas or DoD on-premises	NIPRNet via CAP	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal Systems Strong Virtual Separation Between Tenant Systems & Information	ADP-2 National Agency Check with Law and Credit (NACLC) Non-Disclosure Agreement (NDA)
6	Classified SECRET National Security Systems	Level 5 + Classified Overlay	US / US outlying areas or DoD on-premises CLEARED / CLASSIFIED FACILITIES	SIPRNET DIRECT With DoD SIPRNet Enclave Connection Approval	Virtual / Logical FEDERAL GOV. COMMUNITY Dedicated Multi-Tenant Infrastructure Physically Separate from Non-Federal and Unclassified Systems Strong Virtual Separation Between Tenant Systems & Information	US Citizens w/ Favorably Adjudicated SSBI & SECRET Clearance NDA

MITRE

© 2020 THE MITRE CORPORATION.

25

Slide Source: DoD Cloud Computing Security Requirements Guide, Version 1, Release 3 [7]

### Accreditation Process:

1. FedRAMP - a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services used by the Federal Government.
2. FedRAMP+ - the concept of leveraging the work done as part of the FedRAMP assessment and adding specific security controls and requirements necessary to meet and assure DoD's critical mission requirements.
3. DoD Provisional Authorization (PA) - an acknowledgement of risk based on an evaluation of the CSP's CSO and the potential for risk introduced to DoD networks.

Cloud security information impact levels are defined by the combination of:

- 1) the sensitivity or confidentiality level of information (e.g., public, private, classified, etc.) to be stored and processed in the CSP environment; and
- 2) the potential impact of an event that results in the loss of confidentiality, integrity, or availability of that information.

IL2: Accommodates DoD information that has been approved for public release (Low confidentiality, Moderate Integrity)

IL4: Accommodates DoD Controlled Unclassified Information (CUI) (e.g., FOUO)

IL5: Accommodates DoD CUI and National Security Systems (NSS)

IL6: Accommodates DoD Classified Information up to SECRET

## Cloud-specific Security Challenges



### Today's Top Threats Cloud Security Alliance's Egregious Eleven

1. Data Breaches (1)
2. Misconfiguration and Inadequate Change Control
3. Lack of Cloud Security Architecture and Strategy
4. Insufficient Identity, Credential, Access and Key Management
5. Account Hijacking (5)
6. Insider Threat (6)
7. Insecure Interfaces and APIs (3)
8. Weak Control Plane
9. Metastructure and Applistructure Failures
10. Limited Cloud Usage Visibility
11. Abuse and Nefarious Use of Cloud Services (10)

Slide Source: MITRE

Slide Source: [8]

# MITRE ATT&CK for Cloud

## Cloud Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques. The Matrix contains information for the following platforms: AWS, GCP, Azure, Azure AD, Office 365, SaaS.

[View on the ATT&CK® Navigator](#)

[About the Enterprise domain](#)

[Live Version](#)

layouts ▼ show sub techniques hide sub techniques help

Initial Access 5 techniques	Persistence 5 techniques	Privilege Escalation 1 techniques	Defense Evasion 5 techniques	Credential Access 4 techniques	Discovery 10 techniques	Lateral Movement 2 techniques	Collection 4 techniques	Exfiltration 1 techniques	Impact 4 techniques
Drive-by Compromise Exploit Public-Facing Application Phishing (1) Trusted Relationship Valid Accounts (2)	Account Manipulation (2) Create Account (1) Implant Container Image Office Application Startup (6) Valid Accounts (2)	Valid Accounts (2)	Impair Defenses (1) Modify Cloud Compute Infrastructure (6) Unusual/Unsupported Cloud Regions Use Alternate Authentication Material (2) Valid Accounts (2)	Brute Force (2) Steal Application Access Token Steal Web Session Cookie Unsecured Credentials (3)	Account Discovery (2) Cloud Service Dashboard Cloud Service Discovery Network Service Scanning Network Share Discovery Permission Groups Discovery (1) Remote System Discovery Software Discovery (1) System Information Discovery System Network Connections Discovery	Internal Spearphishing Use Alternate Authentication Material (2)	Data from Cloud Storage Object Data from Information Repositories (2) Data Staged (1) Email Collection (1)	Transfer Data to Cloud Account	Defacement (1) Endpoint Denial of Service (2) Network Denial of Service (2) Resource Hijacking

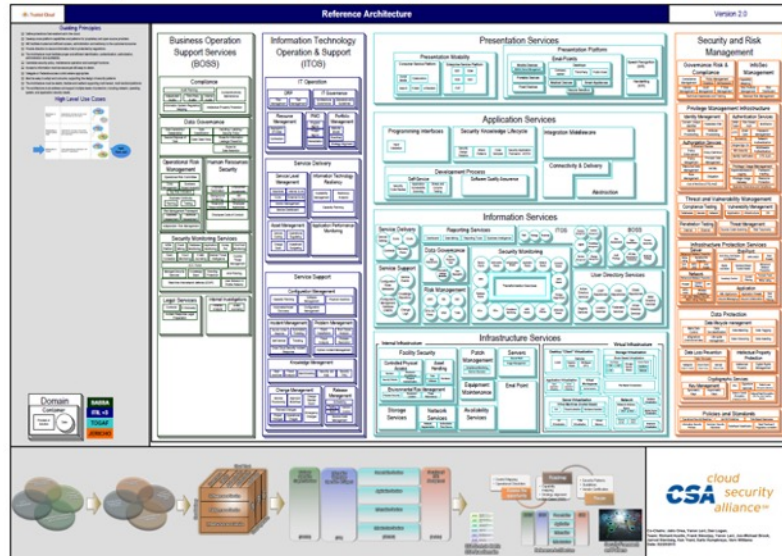
MITRE

© 2020 THE MITRE CORPORATION.

27

Slide Source: <https://attack.mitre.org/matrices/enterprise/cloud/> [9]

# Cloud Security Alliance (CSA) Reference Architecture



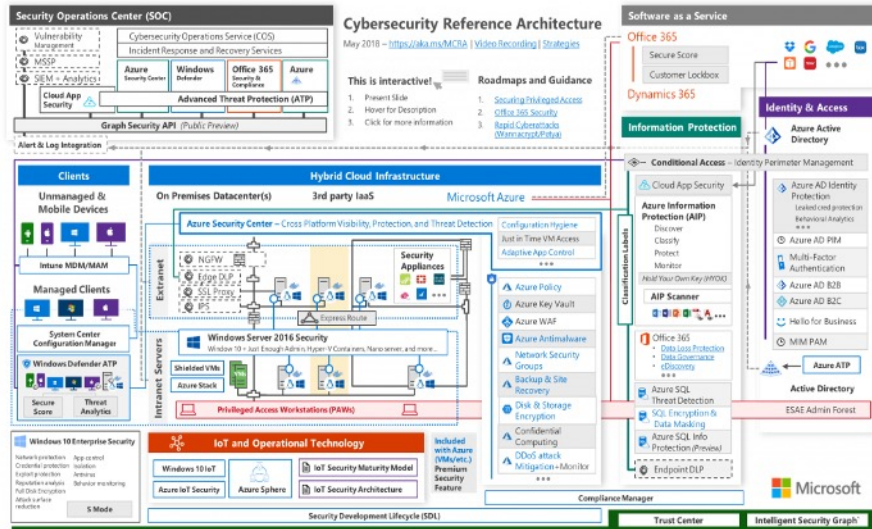
MITRE

© 2020 THE MITRE CORPORATION.

28

Slide Source: Enterprise Architecture v2.0 [10]

# MS Azure Security Architecture



Slide Source: <https://www.microsoft.com/security/blog/2018/06/06/cybersecurity-reference-architecture-security-for-a-hybrid-enterprise/> [11]



## Security Capability Examples

### AWS

**Stateful, Virtual Firewall applied to instance (e.g. EC2)**

- Possible to integrate 3rd party solutions.

**Monitor API Calls through CloudTrail**

- Understand user behavior
- Track resource changes (e.g. creation, modification)

**Monitoring solutions (e.g. CloudTrail) do not provide audit reduction/analysis capabilities. Alternatives:**

- Roll your own
- Integrate capabilities using ELK Stack
- Use CSP products (e.g. Cloudlytics – AWS Cloud Log Analytics & Management Tool)



MITRE

© 2020 THE MITRE CORPORATION.

### Azure

**Virtual Network isolates virtual machines**

**Security posture management through Security Center**

- Automatically deploys monitoring agent into Azure VMs. Manual deployment to on-premises VMs.
- Analytics engines analyze data, provide recommendations and threat alerts
- Aggregate security information into an Azure Monitor workspace or integrate with an existing SIEM.

**Identity and access management through Azure Active Directory (Azure AD)**

- Existing AD organizations use Azure AD Connect to sync identities to the cloud.
- MS365 tenants are automatically Azure AD tenants.



30

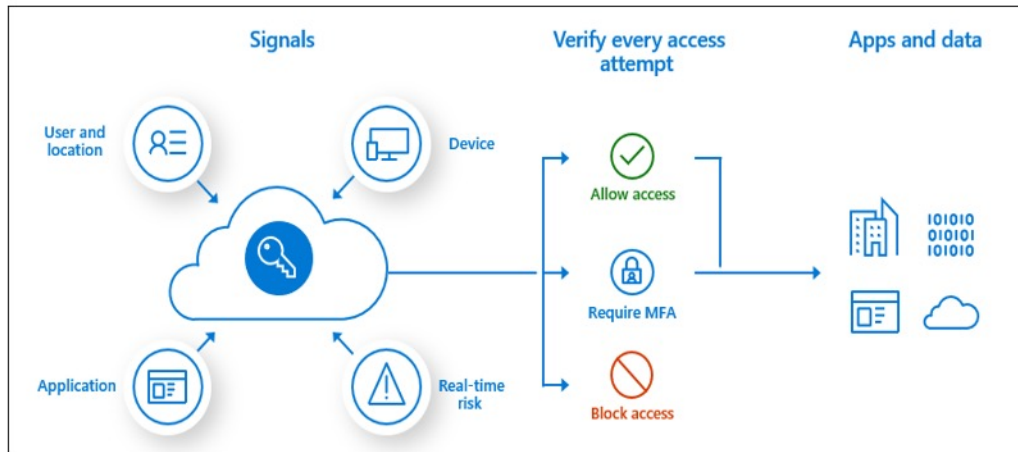
Slide Source: MITRE

Slide Source: <https://azure.microsoft.com/en-us/services/security-center/> [12]

Slide Source: <https://docs.microsoft.com/en-us/azure/security-center/security-center-intro> [13]

Slide Source: <https://docs.microsoft.com/en-in/azure/active-directory/fundamentals/active-directory-compare-azure-ad-to-ad> [14]

## Cloud ZTA (Zero Trust Architecture) – Azure Notional Architecture



MITRE

© 2020 THE MITRE CORPORATION.

31

Slide Source: <https://devblogs.microsoft.com/azuregov/implementing-zero-trust-with-microsoft-azure-identity-and-access-management-1-of-6/> [15]

# Economics

# Cloud Cost Considerations



## **Adoption of cloud services may incur significant costs.**

- Significant migration costs
- Re-engineer applications
- Training/workforce development
- Security monitoring and response
- Absence of a well-crafted exit plan



## **Non-financial benefits should be analyzed as the main drivers for cloud migration.**

- Scalability of computing infrastructure
- Speed of deployment (ONLY IF ATOs are fast)
- Agility in developing new applications
- Data sharing
- Better mission outcome (improved business processes)

Slide Source: MITRE

Katy Warren comment:

**Hosting costs can be enormous if performed incorrectly or based on incorrect assumptions and data, well performed right-sizing is actually rare and difficult; real savings usually occurs when tech refreshes requires purchasing less computers**  
**Use of FFP contracting tends to lead to more expensive cloud costs (i.e., contracting types influence costs)**

**Significant costs include:**

- training everyone on cloud**
- business process changes**
- changes in contractor and CSP contract management practices**
- migration project costs**
- poor acquisitions**
- poor technical architecture**
- security failures**

**Benefits include**

**better mission outcome (improved business processes)**  
**continued tech sustainability and evolution**  
**rapid deployments ONLY IF security can perform ATOs quickly**

## IaaS Cost Drivers

Layer	Non-Recurring Cost	Recurring Cost
Service Management	<ul style="list-style-type: none"> <li>Training</li> </ul>	<ul style="list-style-type: none"> <li>Tier 3 Service Desk</li> <li>Tier 2 Service Desk</li> <li>Request fulfillment</li> <li>Event management</li> <li>Access management</li> <li>Configuration management</li> <li>Continuing security compliance</li> </ul>
Application	<ul style="list-style-type: none"> <li>Modernization / Modification</li> <li>RMF Assessment / ATO</li> <li>Data Migration</li> <li>Parallel operation</li> </ul>	<ul style="list-style-type: none"> <li>Application software license</li> <li>Middleware software license</li> <li>Application and security administration</li> <li>Middleware administration</li> <li>System administration</li> </ul>
Common Services	<ul style="list-style-type: none"> <li>Development</li> <li>RMF Assessment / ATO</li> </ul>	<ul style="list-style-type: none"> <li>Sustainment</li> <li>Cyber Security Service Provider (CSSP)</li> </ul>
Connectivity	<ul style="list-style-type: none"> <li>Connection fee</li> </ul>	<ul style="list-style-type: none"> <li>Connection</li> <li>Data transport</li> </ul>
<b>Infrastructure-as-a-Service (IaaS)</b>	<ul style="list-style-type: none"> <li>Acquisition cost</li> </ul>	<ul style="list-style-type: none"> <li>Cloud Services</li> </ul>

IaaS eliminates hardware and facilities cost and reduces system admins cost

Slide Source: MITRE

## PaaS Cost Drivers

Layer	Non-Recurring Cost	Recurring Cost
Service Management	<ul style="list-style-type: none"> <li>• Training</li> </ul>	<ul style="list-style-type: none"> <li>• Tier 3 Service Desk</li> <li>• Tier 2 Service Desk</li> <li>• Request fulfillment</li> <li>• Event management</li> <li>• Access management</li> <li>• Configuration management</li> <li>• Continuing security compliance</li> </ul>
Application	<ul style="list-style-type: none"> <li>• Modernization / Modification</li> <li>• RMF Assessment / ATO</li> <li>• Data migration</li> <li>• Parallel operation</li> </ul>	<ul style="list-style-type: none"> <li>• Application software license</li> <li>• Application and security administration</li> </ul>
Common Services	<ul style="list-style-type: none"> <li>• Development</li> <li>• RMF Assessment / ATO</li> </ul>	<ul style="list-style-type: none"> <li>• Sustainment</li> <li>• Cyber Security Service Provider (CSSP)</li> </ul>
Connectivity	<ul style="list-style-type: none"> <li>• Connection fee</li> </ul>	<ul style="list-style-type: none"> <li>• Connection</li> <li>• Data transport</li> </ul>
<b>Platform-as-a-Service (PaaS)</b> <ul style="list-style-type: none"> <li>• Acquisition cost</li> <li>• Cloud Services</li> </ul>		

PaaS eliminates hardware, facilities, and system admins cost; reduces cost of middleware admins and software licenses

Slide Source: MITRE

## SaaS Cost Drivers

Layer	Non-Recurring Cost	Recurring Cost
Service Management	<ul style="list-style-type: none"> <li>• RMF Assessment / ATO</li> <li>• Data migration</li> <li>• Parallel operation</li> <li>• Training</li> </ul>	<ul style="list-style-type: none"> <li>• Tier 2 Service Desk</li> <li>• Request fulfillment</li> <li>• Event management</li> <li>• Access management</li> <li>• Configuration management</li> <li>• Continuing security compliance</li> <li>• CSSP Fee</li> </ul>
Connectivity	<ul style="list-style-type: none"> <li>• Connection fee</li> </ul>	<ul style="list-style-type: none"> <li>• Connection</li> <li>• Data transport</li> </ul>
<b>Software-as-a-Service (SaaS)</b>	<ul style="list-style-type: none"> <li>• Acquisition cost</li> </ul>	<ul style="list-style-type: none"> <li>• Cloud Services (includes Tier 3 Service Desk)</li> </ul>

SaaS eliminates hardware, facilities, software licenses, and admin costs; and reduces support requirement

Slide Source: MITRE



## Cost Calculators – Hosting

**AWS**

The screenshot shows the 'Configure Amazon EC2' page in the AWS Cost Calculator. It includes sections for 'Region', 'Instance profile', 'EC2 instance specifications', and 'Workload'. The workload section features four graphs: 'Constant', 'Periodic', 'Variable', and 'Peak', each with a corresponding line graph showing different usage patterns over time.

**Azure**

The screenshot shows the 'Your Estimate' page in the Azure Cost Calculator for Virtual Machines. It includes sections for 'Virtual Machines', 'Savings Options', and 'Compute (D2V6)'. The 'Virtual Machines' section shows a table with columns for 'VM size', 'VM type', 'VM family', and 'VM size'. The 'Savings Options' section includes a 'Savings plan' dropdown and a 'Savings plan' button. The 'Compute (D2V6)' section shows a table with columns for 'VM size', 'VM type', 'VM family', and 'VM size'. The total cost is displayed as '\$37.02'.

**CAUTION: Tools are only as good as the user's knowledge and the data available**

Slide Source: AWS: <https://calculator.aws/#/addService> [16]

Slide Source: Azure: <https://azure.microsoft.com/en-us/pricing/calculator/> [17]

# Workforce Development

## Cloud's Culture Shift

### Buying to Renting

Move from designing solutions to defining needs

CAPEX → OPEX

### New Skills or Organizations

Tech Skills

Acquisition & CSP Contract Management

Cloud Security

Continuous Improvement

### New Approaches

Acquisition

Contracting

Technology Development (DevSecOps)

Security

Slide Source: MITRE

## Workforce Strategy, Cloud Smart



### Identify Skill Gaps for Current and Future Work Roles

- Conduct a skills gap analysis that maps current IT workforce resources to future skill and position requirements.
- Leverage industry projections to help predict future workforce skill and position requirements, especially for IT roles.



### Reskill and Retain Current Employees

- Account for technical as well as non-technical (acquisition) needs.
- Leaders actively back the effort and remove roadblocks.



### Recruit and Hire to Address Skill Gaps

- Expand the use of pay flexibilities and remove bureaucratic barriers to hiring staff expeditiously.
- Build a talent pipeline to expand the pool of qualified applicants.



### Employee Communication, Engagement, and Transition Strategies

- Clearly articulate how the current workforce will align once cloud adoption is complete.
- Socialize a technology roadmap and the change management process to include reskilling opportunities.

Slide Source: <https://cloud.cio.gov/strategy/> [18]

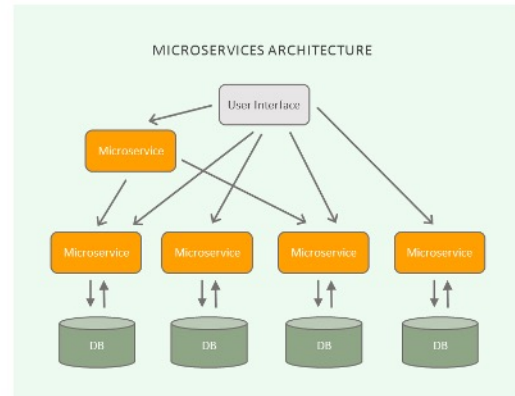
# Cloud DevSecOps

## Microservices

Microservices – a **cloud native** architectural approach in which a single application is composed of many loosely coupled and independently deployable smaller components, or services.

Key Advantages:

- **Horizontal Scaling** – If one service is under heavy load, run more replicas of that particular service.
- **Service Independence** – Each component can live in a separate repository and be maintained by a dedicated team of engineers. The component is written in the language best suited for its purpose, so a database service might be written in C and the web server in Python.
- **Pluggable Architecture** – An organization does not need to write all of its services. Third party applications like MySQL, Elasticsearch, Redis are all microservices that can be integrated into systems.
- **Fault Tolerance** - The failure of one replica of a service should not cause the whole pipeline or even that service to fail.



Slide Source: <https://www.ibm.com/cloud/learn/microservices> [19]

Slide Source: <https://hackernoon.com/how-microservices-saved-the-internet-30cd4b9c6230> [20]

Microservices Image: <https://hackernoon.com/how-microservices-saved-the-internet-30cd4b9c6230>

Microservices are not necessarily exclusively relevant to cloud computing but there are a few important reasons why they so frequently go together—reasons that go beyond microservices being a popular architectural style for new applications and the cloud being a popular hosting destination for new applications.

## Containers, Docker, and Kubernetes



### Containers

Unlike a Virtual Machine (VM) containers virtualize the operating system, rather than the physical hardware.

#### Benefits:

- Lightweight – quickly scale up **cloud-native** applications.
- Portable and platform independent – write software once and run
- Supports modern development and architecture, such as DevSecOps and microservices
- Improves CPU and memory utilization



By far the most popular containerization platform. ('Docker' and 'containers' are used interchangeably.)

#### Enables:

- Automated container creation – build a container based on application source code
- Container reuse via base images
- Shared container libraries – devs can access an open-source registry containing thousands of user-contributed containers.



### kubernetes

Kubernetes is a container orchestration platform for containerized applications.

#### Schedules and automates:

- Container deployment
- Service discovery (DNS/public IP)
- Storage provisioning
- Load balancing and scaling
- Self-healing for high availability

Slide Source: <https://www.ibm.com/cloud/learn/microservices> [19]

Container image: <https://archive.turbonomic.com/wp-content/uploads/2014/04/ContainerIconBlue-min.jpg>

Docker image: <https://www.docker.com/company/newsroom/media-resources>

Kubernetes image: [https://blogs.vmware.com/cloudnative/files/2017/12/1024px-Kubernetes\\_logo.svg\\_-1024x181.png](https://blogs.vmware.com/cloudnative/files/2017/12/1024px-Kubernetes_logo.svg_-1024x181.png)

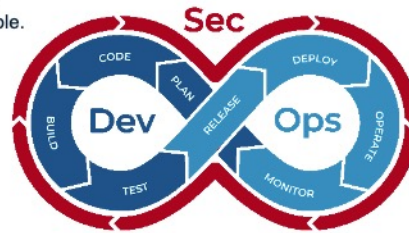
## DevSecOps Methodologies, Principles, and Strategies

**Continuous integration (CI)** – members of a team use a version control system and frequently integrate their work to the same location, such as a main branch. Each change is built and verified (tested) to detect integration errors as quickly as possible.

**Continuous delivery (CD)** – Every software change is automatically built, tested, and deployed to production.

### **Implement:**

- Auditability – ensure compliance with security controls
- Visibility – monitoring system in place to measure the heartbeat of the operation, send alerts, increase awareness of changes and cyberattacks



**Shift left** – move security from the right (end) to the left (beginning) of the DevOps (delivery) process

**Accelerate** the delivery of reliable software

**Balance** speed, cost, quality, and risk with increased capacity to innovate

**Reduce** time to user feedback with improved user experience

**Continually experiment** to encourage risk-taking and learn from success and failure

**Incentivize** development, test, and deployment teams to collaborate on shared goals

MITRE

© 2020 THE MITRE CORPORATION.

44

Slide Source: <https://docs.aws.amazon.com/codepipeline/latest/userguide/concepts-continuous-delivery-integration.html> [21]

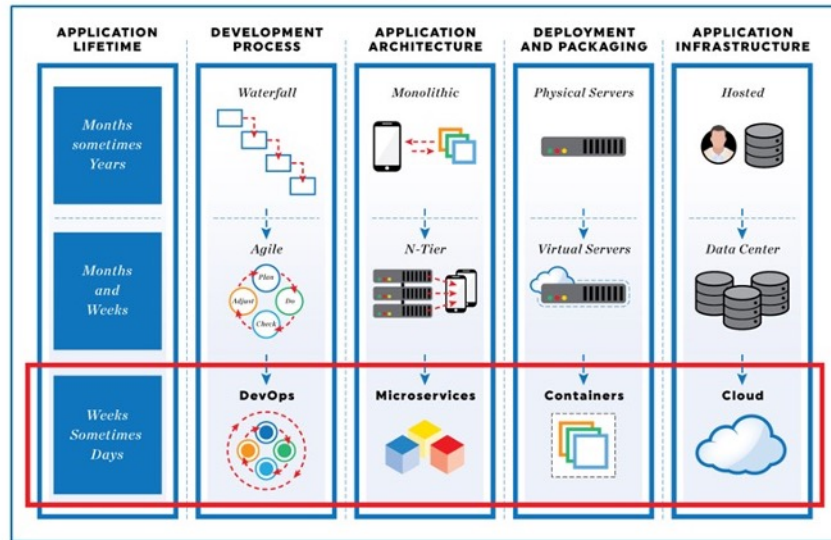
Slide Source: <https://www.ibm.com/cloud/learn/devops-a-complete-guide> [22]

Slide Source: <https://www.ibm.com/cloud/learn/devsecops> [23]

DevSecOps image: [https://sasg.arizona.edu/sites/default/files/devsecops\\_diagram.png](https://sasg.arizona.edu/sites/default/files/devsecops_diagram.png)



## From Waterfall to DevSecOps

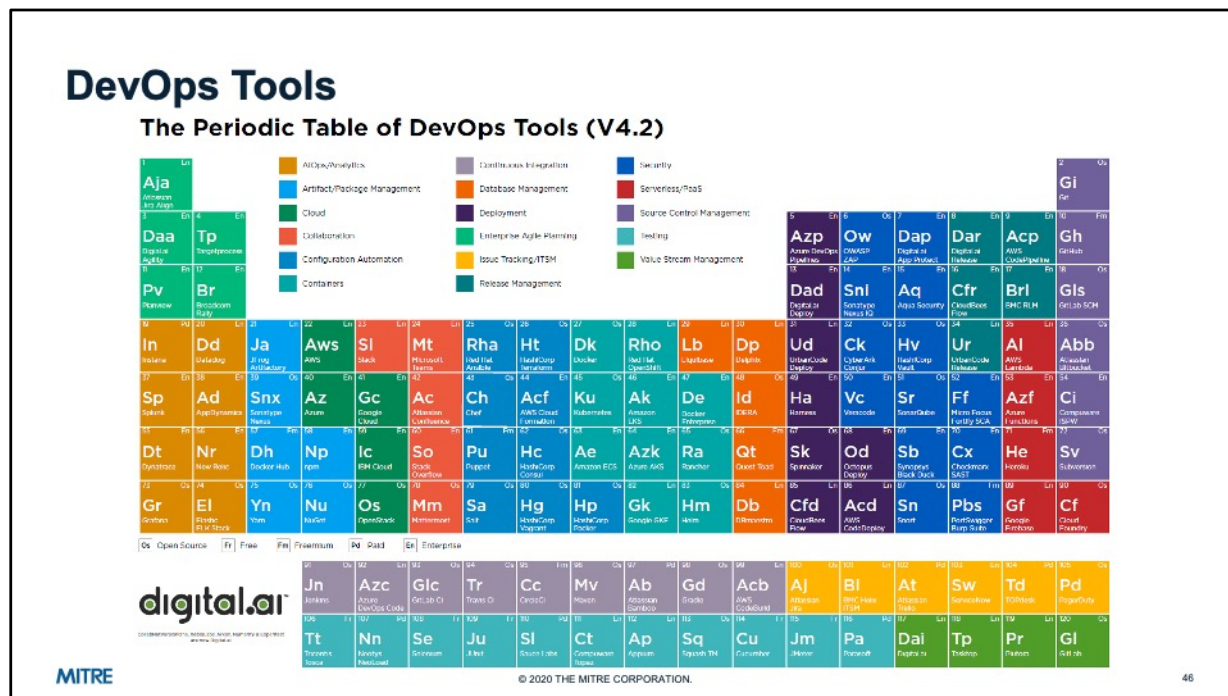


MITRE

© 2020 THE MITRE CORPORATION.

45

Slide Source: DoD Enterprise DevSecOps Initiative (Software Factory) [24]



Slide Source: <https://digital.ai/periodic-table-of-devops-tools> [25]

The Periodic Table of DevOps Tools is the industry's go-to resource for identifying best-of-breed tools across the software delivery lifecycle.

**Created by DevOps practitioners for DevOps practitioners**, over 18,000 votes were cast across more than 400 products in 17 categories to produce the 2020 Periodic Table of DevOps Tools.

Whether you are starting fresh, filling gaps, or replacing existing DevOps tools, get started by using Periodic Table to identify the right tools for your DevOps pipeline.

## References

- [1] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," Computer Security Division, Information Technology Laboratory, Gaithersburg, MD, 2011.
- [2] H. A. Terry, "Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services," Department of Defense, 2014.
- [3] Department of Defense, "DoD Cloud Strategy," 2018.
- [4] Defense Information Systems Agency, "DISA Cloud Playbook," 2018.
- [5] Amazon Web Services, "An Overview of the AWS Cloud Adoption Framework, Version 2," 2017.
- [6] Microsoft, "Microsoft - About the Microsoft Cloud Adoption Framework," [Online]. Available: <https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/overview>. [Accessed 29 September 2020].
- [7] Defense Information Systems Agency, "Department of Defense Cloud Computing Security Requirements Guide, Version 1, Release 3," 2017.
- [8] Cloud Security Alliance, "Top Threats to Cloud Computing, The Egregious 11," Cloud Security Alliance, 2020.
- [9] MITRE, "MITRE ATT&CK Cloud Matrix," 2 July 2020. [Online]. Available: <https://attack.mitre.org/matrices/enterprise/cloud/>. [Accessed 30 September 2020].
- [10] Cloud Security Alliance, "Enterprise Architecture v2.0," 25 February 2013. [Online]. Available: <https://cloudsecurityalliance.org/artifacts/tci-reference-architecture-v2-0/>. [Accessed 30 September 2020].
- [11] Microsoft, "Cybersecurity Reference Architecture: Security for a Hybrid Enterprise," 6 June 2018. [Online]. Available: <https://www.microsoft.com/security/blog/2018/06/06/cybersecurity-reference-architecture-security-for-a-hybrid-enterprise/>. [Accessed 30 September 2020].
- [12] Microsoft, "Azure Security Center," 30 September 2020. [Online]. Available: <https://azure.microsoft.com/en-us/services/security-center/>.
- [13] Microsoft, "What is Azure Security Center?," 22 September 2020. [Online]. Available: <https://docs.microsoft.com/en-us/azure/security-center/security-center-introduction>. [Accessed 30 September 2020].
- [14] Microsoft, "Compare Active Directory to Azure Active Directory," 26 February 2020. [Online]. Available: <https://docs.microsoft.com/en-in/azure/active-directory/fundamentals/active-directory-compare-azure-ad-to-ad>. [Accessed 1 October 2020].
- [15] T. Banasik, "Implementing Zero Trust with Microsoft Azure: Identity and Access Management (1 of 6)," Microsoft, 21 January 2020. [Online]. Available: <https://devblogs.microsoft.com/azuregov/implementing-zero-trust-with-microsoft-azure-identity-and-access-management-1-of-6/>. [Accessed 30 September 2020].
- [16] Amazon Web Services, "Pricing Calculator," [Online]. Available: <https://calculator.aws/#/addService>. [Accessed 30 September 2020].
- [17] Microsoft, "Pricing calculator," [Online]. Available: <https://azure.microsoft.com/en-us/pricing/calculator/>. [Accessed 30 September 2020].
- [18] Office of the Federal Chief Information Officer, "From Cloud First to Cloud Smart," [Online]. Available: <https://cloud.cio.gov/strategy/>. [Accessed 30 September 2020].
- [19] IBM, "Microservices," [Online]. Available: <https://www.ibm.com/cloud/learn/microservices>. [Accessed 30 September 2020].
- [20] Hackernoon, "How Microservices Saved the Internet," [Online]. Available: <https://hackernoon.com/how-microservices-saved-the-internet-30cd4b9c6230>. [Accessed 30 September 2020].
- [21] Amazon Web Services, "Continuous delivery and continuous integration," [Online]. Available: <https://docs.aws.amazon.com/codepipeline/latest/userguide/concepts-continuous-delivery-integration.html>. [Accessed 30 September 2020].
- [22] IBM, "DevOps," [Online]. Available: <https://www.ibm.com/cloud/learn/devops-a-complete-guide>. [Accessed 30 September 2020].
- [23] IBM, "DevSecOps," [Online]. Available: <https://www.ibm.com/cloud/learn/devsecops>. [Accessed 30 September 2020].
- [24] N. Chaillan, "DoD Enterprise DevSecOps Initiative (Software Factory)," US Air Force.
- [25] digital.ai, "Periodic Table of DevOps Tools," [Online]. Available: <https://digital.ai/periodic-table-of-devops-tools/>. [Accessed 30 September 2020].
- [26] D. Shackleford, "SANS 2019 Cloud Security Survey," SANS Institute, 2019.
- [27] Amazon Web Services, "Shared Responsibility Model," [Online]. Available: <https://aws.amazon.com/compliance/shared-responsibility-model/>. [Accessed 30 September 2020].

MITRE

© 2020 THE MITRE CORPORATION.

# Backup

## Most Used Government Community Clouds



### AWS GovCloud (US)

- Isolated AWS Regions designed to allow U.S. government agencies and customers to move sensitive workloads into the cloud by addressing their specific regulatory and compliance requirements, including FedRAMP High; DoD SRG IL5,6 Level 5; CJIS; and ITAR requirements
- Physical and logical administrative access to AWS personnel that are U.S. citizens only
- Providing FIPS 140-2 endpoints



### Azure Government

- Azure Government delivers a dedicated cloud enabling government agencies and their partners to transform mission-critical workloads to the cloud
- Azure Government services handle data that is subject to certain government regulations and requirements, such as FedRAMP High; SRG L5, L6; ITAR: IRS 1075; and CJIS\
- Azure Government uses physically isolated datacenters and networks (located in U.S. only)
- Regions and Availability zones



### Google Cloud

- Google Cloud Platform (GCP) has a FedRAMP High ATO for 17 products in 5 regions and maintains a Moderate (P-ATO) for 64 Products in 20 regions. Additionally G Suite has FedRAMP
- Google has an IL2 authorization for G Suite and GCP
- Emphasis on serverless computing, big data analytics, machine learning, and artificial intelligence. Largest storage customer has 250+ Petabytes of data

MITRE

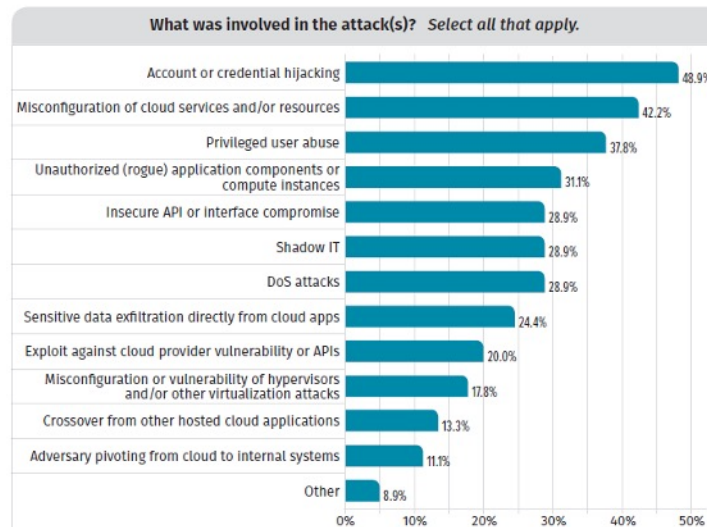
© 2020 THE MITRE CORPORATION.

Note: Data Provided by CSPs

Slide Source: MITRE

IBM and Oracle are other commonly used Commercial Government Clouds. Provisional Authority to Operate (P-ATO)

## Cloud Attacks – SANS 2019 Cloud Security Survey Tactics



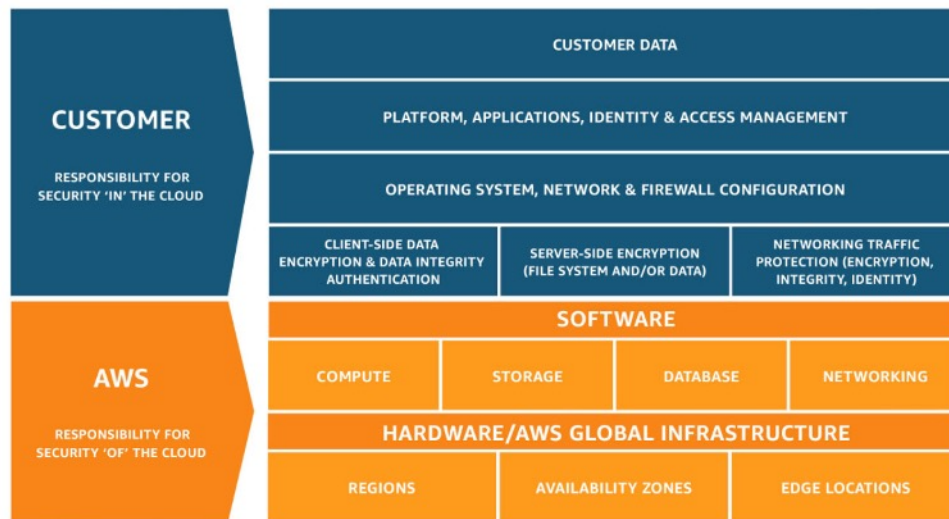
MITRE

© 2020 THE MITRE CORPORATION.

50

Slide Source: [26]

## Shared Security Responsibility (Example - AWS)



Slide Source: <https://aws.amazon.com/compliance/shared-responsibility-model/> [27]



## Cloud One



Air Force Cloud Office with turnkey access to AWS GovCloud and Azure Government at IL2, 4 and 5. IL6 available by December 2019.

Simple "Pay per use" model with ability to instantiate your own Development and Production VPCs at various Impact Levels within days with full compliance/security and a baked-in ATO.

Enterprise Solution: we provide the guardrails to the cloud in a standard manner so you can focus on your mission

Fully Automated: All environmental stand-up is managed by Infrastructure as Code, drastically speeding up deployment, reducing manual work, and human error

Centralized Identities and Single-Sign-On (SSO): one login across the Cloud stack

Internet facing Cloud based VPN to connect to IL5 enclaves with a Virtual Internet Access Point (coming within January 2020).

DevSecOps Focused: secure, mission driven deployments are built into the framework to ensure self-service and seamless deployments. Leverages Zero Trust model.

Proactive Scaling and System Monitoring: Mission Owners can see all operational metrics and provide rules and alerts to manage each mission their way

Accreditation Inheritance has been identified in the AF-Cloud One eMASS accounts (AWS & Azure) to include inheritance from the CSP, USAF, DoD and CSSP. All that's left for the mission is the controls that are unique to them.

Slide Source: DoD Enterprise DevSecOps Initiative (Software Factory) [24]



**MITRE** | SOLVING PROBLEMS  
FOR A SAFER WORLD™

© 2020 THE MITRE CORPORATION.