SCSS 2019
Software and Cyber Solutions Symposium: Benefits and Risks of Cloud Computing

Implementing and Updating Cloud Computing Best Practices

Nathaniel Richmond

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Implementing and Updating Cloud Computing Best Practices

Document Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM19-0900

Updating the Distribution Statement

To appropriately update the distribution markings in the footer of your presentation, follow these steps:

1. From the *Home* tab, select *Replace* at the right side of the tool bar.
2. Paste "[DISTRIBUTION STATEMENT Please copy and paste the appropriate distribution statement into this space.]" in the *Find what* field.
3. Paste a short version of the distribution statement provided by the Document Marking System (e.g., [DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.]), with brackets around it, in the *Replace with* field. See the table on the next slide for the short statements you can use. (If you have questions, send email to DMARR-Team@sei.cmu.edu.)
4. Click the *Replace All* button. Voilà! You're done!

You can use this same *Replace* command to update the title, date, and copyright of your presentation without having to access slide master pages.

Short Distribution Statements

Statement in Document Markings System	Short Statement You Can Use
[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution.	[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.
[DISTRIBUTION STATEMENT B] Distribution authorized to U.S. Government Agencies only (fill in reason) (date of determination). Other requests for this document shall be referred to (insert controlling DoD office).	[DISTRIBUTION STATEMENT B] U.S. Government Agencies only.
[DISTRIBUTION STATEMENT C] Distribution authorized to U.S. Government Agencies and their contractors (fill in reason) (date of determination). Other requests for this document shall be referred to (insert controlling DoD office).	[DISTRIBUTION STATEMENT C] U.S. Government Agencies and their contractors only.
[DISTRIBUTION STATEMENT D] Distribution authorized to the Department of Defense and U.S. DoD contractors only (fill in reason) (date of determination). Other requests shall be referred to (insert controlling DoD office).	[DISTRIBUTION STATEMENT D] Department of Defense and U.S. DoD contractors only.
[DISTRIBUTION STATEMENT E] Distribution authorized to DoD Components only (fill in reason) (date of determination). Other requests shall be referred to (insert controlling DoD office).	[DISTRIBUTION STATEMENT E] DoD Components only.
[DISTRIBUTION STATEMENT F] Further dissemination only as directed by (inserting controlling DoD office) (date of determination) or higher DoD Authority.	Keep the entire statement. There is no short statement you can use.
[INTERNAL SEI-USE ONLY] Further dissemination requires re-submittal through DM-RRO.	[INTERNAL SEI-USE ONLY] DM-RRO REQUIRED.
[FUNDAMENTAL RESEARCH] This material was created under project [FR ID]; DFARS 252.204-7000 does not apply.	[FR ID]; DFARS 252.204-7000 does not apply.

Agenda

Introduction

Recap of previous work

Volatility of cloud services

Methods to stay current

Translating to best practices and implementation

Implementing and Updating Cloud Computing Best Practices

Introduction

Introduction

- Read my bio if you want
  - Started in IT
  - Worked cybersecurity operations and incident response
  - Team lead, Security Solutions, part of Monitoring and Response within CERT.
    - Architecture
    - Cybersecurity operations
    - Transitioning research to practice

I do not consider myself an expert at cloud computing, so this presentation is an effort to show, in part, how I work towards the knowledge I need.

Introduction: “Must know AWS”

https://twitter.com/anildash/status/955476924402487296

Implementing and Updating Cloud Computing Best Practices

Recap of previous work

Previous Work: Overview of Risks, Threats, and Vulnerabilities Faced in Moving to the Cloud

1. Consumers Have Reduced Visibility and Control
2. On-Demand Self Service Simplifies Unauthorized Use
3. Internet-Accessible Management APIs can be Compromised
4. Separation Among Multiple Tenants Fails
5. Data Deletion is Incomplete
6. Credentials are Stolen
7. Vendor Lock-In Complicates Moving to Other CSPs
8. Increased Complexity Strains IT Staff
9. Insiders Abuse Authorized Access
10. Stored Data is Lost
11. CSP Supply Chain is Compromised
12. Insufficient Due Diligence Increases Cybersecurity Risk

Previous Work: Cloud Security Best Practices

- Due Diligence
  - Planning
  - Development and Deployment
  - Operation
  - Decommissioning
  - Multiple-CSP Strategy
- Managing Access
  - Identify and Authenticate Users
  - Assign User Access Rights
  - Create and Enforce Resource Access Policies
- Protect Data
  - Protect From Unauthorized Access
  - Ensure Availability of Critical Data
  - Prevent Disclosure of Deleted Data
- Monitor and Defend
  - Monitor Cloud-Deployed Resources
  - Analyze Both Cloud and On-Premise Monitoring
  - Coordinate with CSP

Previous Work: Operation Cloud Hopper Case Study

A blog post to try and show how one could use the guidance from the previous two documents to identify and mitigate risk.

Related risks, threats, and vulnerabilities from previous report:

- Consumers have reduced visibility and control
- Credentials are stolen – Easy example of something that can be mitigated, i.e. multi-factor auth (MFA)
- Increased complexity strains IT staff
- Insiders abuse authorized access
- Insufficient due diligence increases risk

Additional potential for risks, threats, or vulnerabilities

- Risk from one customer can transfer to another
- Traditional risks, threats, and vulnerabilities

Implementing and Updating Cloud Computing Best Practices

Volatility of cloud services

Example of Industry Volatility

The following are just a couple key examples that have changed since the previous papers were written.

1. AWS Site-toSite VPN now supports certificate authentication instead of just pre-shared keys: https://aws.amazon.com/about-aws/whats-new/2019/08/aws-site-to-site-vpn-now-supports-certificate-authentication/
2. Azure Kubernetes Service (AKS) supports egress filtering (or maybe not?): https://docs.microsoft.com/en-us/azure/aks/limit-egress-traffic
3. Don’t forget cost forecasting

Volatility Examples – Continued

Government clouds are different than the commercial offerings, both at a high level and sometimes in the details. Some services behave differently, some are released at different times, and more.

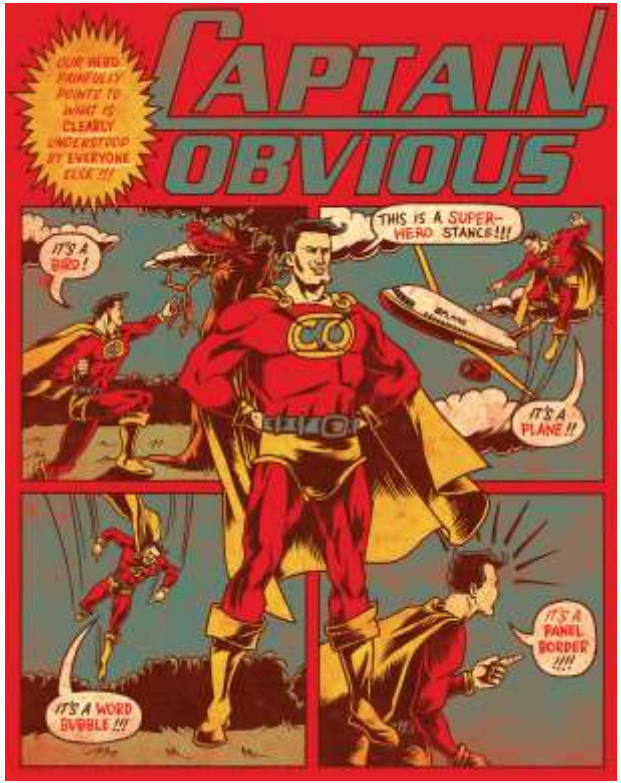
Examples:

- AWS
  - GovCloud S3 namespaces are regional, not global
  - Three GovCloud S3 endpoints, two for ITAR and one for FIPS
- Azure
  - User activity in Security Center not logged in Azure Government
  - URLs for API Management are different

Implementing and Updating Cloud Computing Best Practices

Methods to stay current

Methods to stay current: Vendors



Most vendors have multiple ways to propagate information about changes to their services, including:

- Website
- Twitter and other social media

They will usually notify customers of:

- New products and services
- End of life products and services
- Changes to products and services

Methods to stay current: Hands-on

There is no substitute to use a product or service day-to-day. Your knowledge will always be better, all other things being equal.

- Work lab
- Customer lab
- Production
- Other (personal projects or experimentation, class-based, etc)

Note that, if you have the opportunity for hands-on work, that also means you likely have potential mentors at your organization that could help you learn. I have a number of colleagues across the CERT Division and SEI that I know can help me at the strategic level down to the technical details.

Methods to stay current: Formal training

Formal training generally has a few positives and a few negatives compared to self-taught or on-the-job training.

Potential positives:

1. Some people learn better in a classroom environment
2. It removes you from the day-to-day to allow focus
3. Usually includes a mix of lecture and hands-on lab material – you should probably avoid anything without labs
4. Could cover material that you don't get to use as much in practice

Potential negatives:

1. Usually expensive
2. Easy to lose what you learned if you don't use it afterward

Methods to stay current: Industry experts, policies and regulations, government resources

Industry Experts:

- Research firms
- Companies (for profit and non-profit)
- Individuals and other resources like flaws.cloud and flaws2.cloud

Policies and regulations:

- FIPS
- ITAR
- GDPR

Government resources

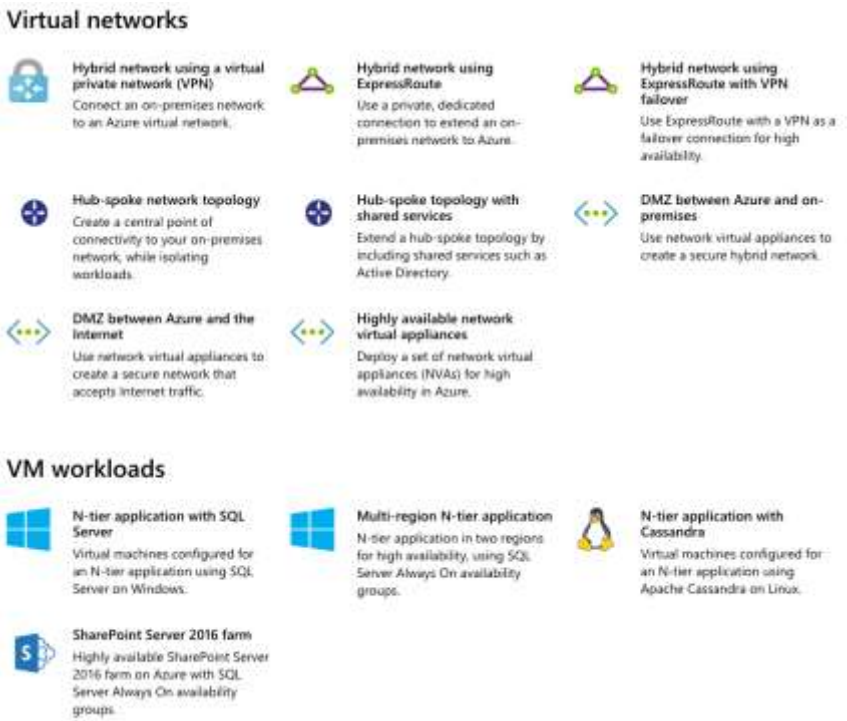
- FedRAMP

Implementing and Updating Cloud Computing Best Practices

Translating to best practices and implementation

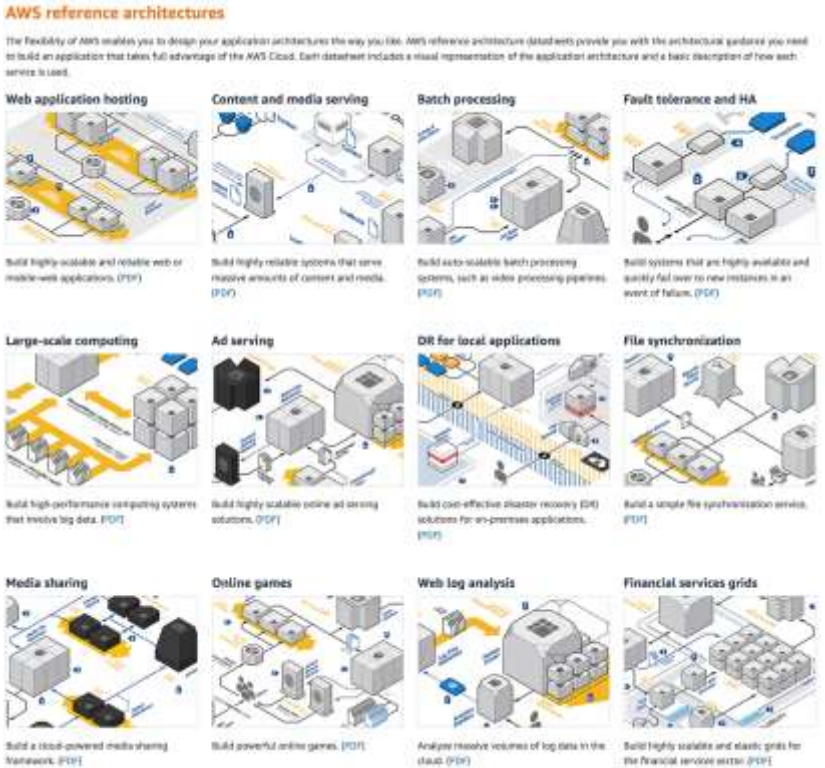
Transitioning best practices: Industry and vendor examples

- Reference models, frameworks, and other examples help you break down the problem based on vendor guidance
- Reference architecture examples:
  - AI/ML
  - Big data
  - IoT
  - Serverless
  - Virtual networks
  - VM workloads
  - Web applications
  - More…



Transitioning best practices: Industry and vendor examples

- Working templates and implementations
  - AWS Quick Starts with CloudFormation
  - GCP Deployment Manager samples on Github
  - Azure Resource Manager Quickstart Templates
  - Some vendors can use this as a differentiator from competition



Transitioning best practices: Manageable chunks

It can be difficult to take a high-level best practice like, “Protect data from unauthorized access,” and implement it. Decompose the practice into manageable chunks.

An example of breaking this one into a few steps:

1. Identify data types and sensitivity
2. Determine mechanisms for authentication and access control, which will change depending on cloud model (hybrid, native) and how it is integrated with local infrastructure
3. Determine roles for different levels of access, put users in appropriate roles
4. Make sure defaults are secure!
5. Feed into risk management, vulnerability, and other processes (e.g. identify a potential issue like SSRF and mitigate if possible)
6. Iterate through steps to identify what is missing or further decompose into actions

Transitioning best practices: CI/CD and DevOps

DevOps

"DevOps is a software development approach that brings development and operations staff (IT) together." Focuses on agility and automation.

https://insights.sei.cmu.edu/sei_blog/2014/11/a-new-weekly-blog-series-to-help-organizations-adopt-implement-devops.html

SEI DevOps blog contains a wealth of information going back years.

https://insights.sei.cmu.edu/devops/

Secure DevOps

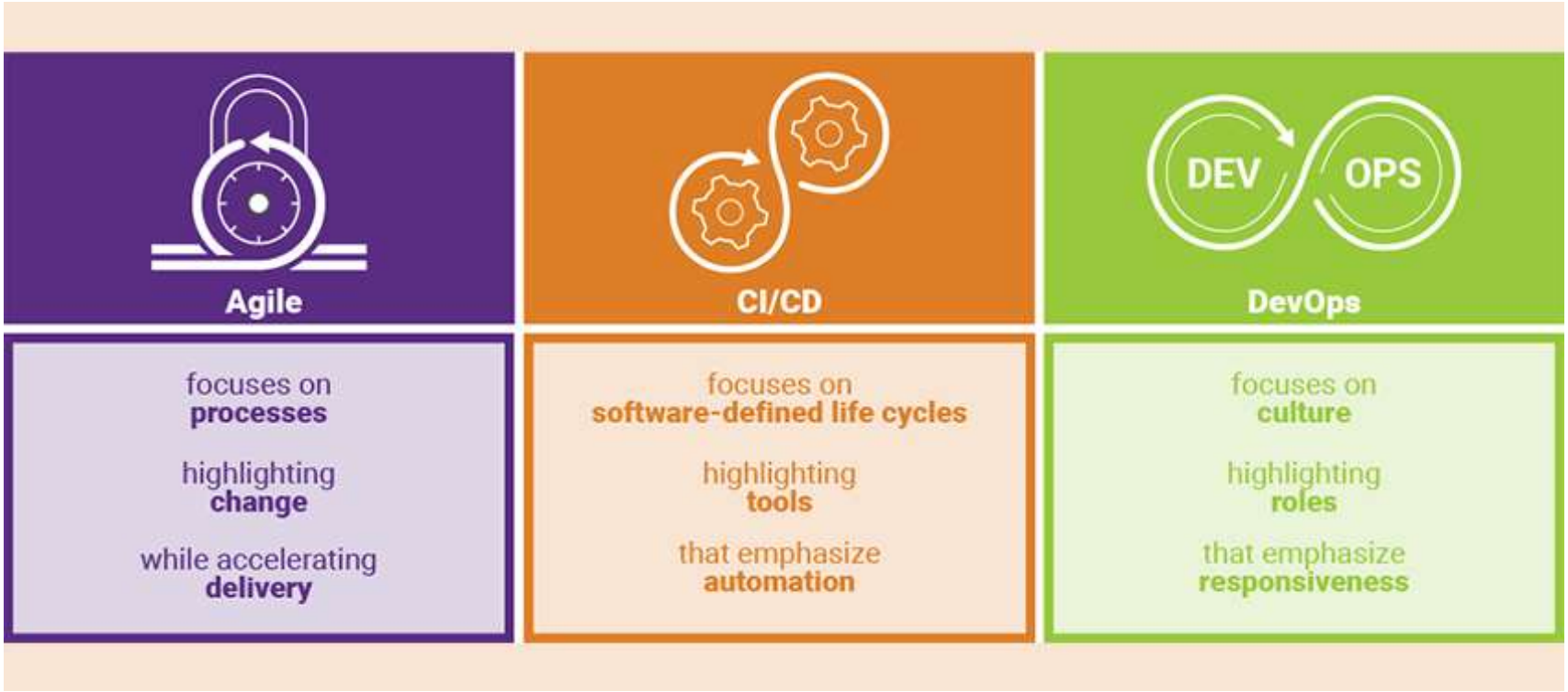
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=465551

Continuous Integration/Continuous Delivery (CI/CD)

CI is frequent build and test, CD is delivering the code from one environment to another.

https://insights.sei.cmu.edu/devops/2015/09/-a-devops-a-day-keeps-the-auditors-away-and-helps-organizations-stay-in-compliance-with-federal-regu.html

Transitioning best practices: CI/CD and DevOps



https://www.synopsys.com/blogs/software-security/agile-cicd-devops-difference/

Conclusion

Contact Information

Presenter / Point of Contact match to Information Sheets

Nathaniel Richmond

Senior Team Lead

Telephone: +1 703.247.1395

Email: nr@cert.org