Carnegie Mellon University
Software Engineering Institute

Cloud Security

JUNE 7, 2023

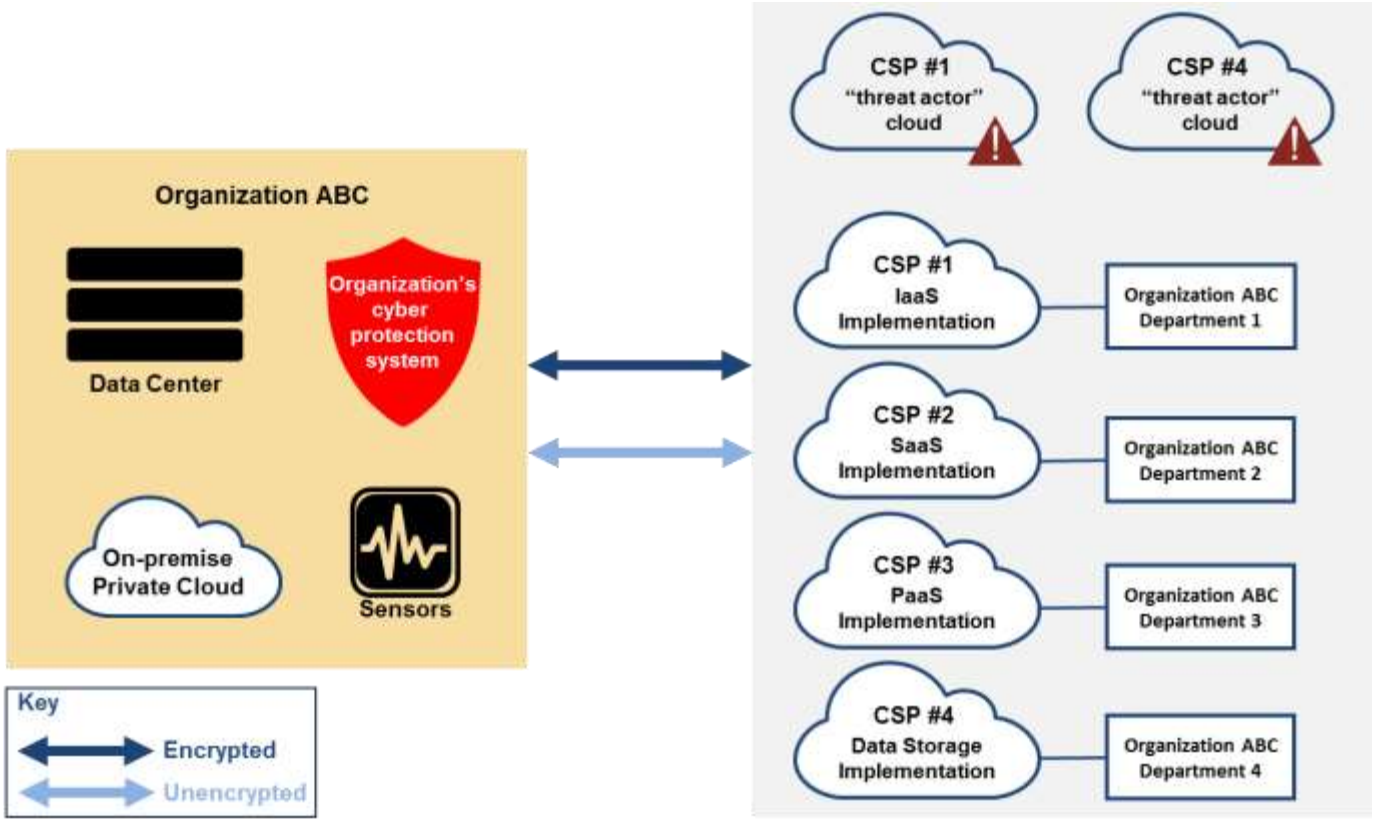
Tim Morrow
CMU/SEI CERT Situational Awareness Technical Manager

Document Markings

Cloud Threats and Risks

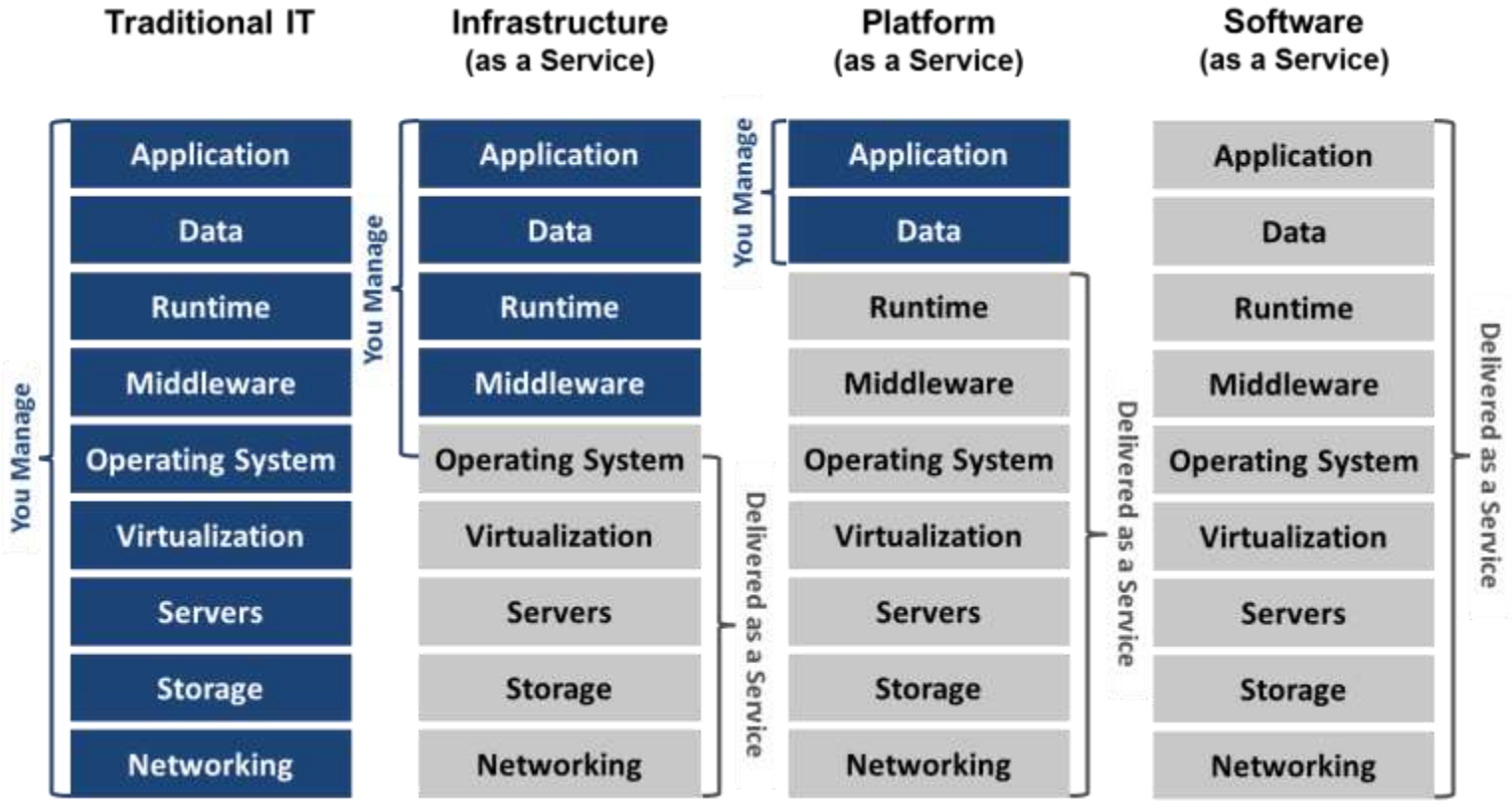
Carnegie Mellon University
Software Engineering Institute

Hybrid Cloud Environment



Cloud service provider (CSP)

Shared Responsibility Model



Cloud-Unique Threats and Risks

1. Reduced Visibility and Control
2. On-Demand Self Service Simplifies Unauthorized Use
3. Management Application Programming Interface (API) Compromise
4. Logical Separation Failure Among Multiple Tenants
5. Incomplete Data Deletion

Cloud and On-Premise Threats and Risks

1. Stolen Credentials
2. Vendor Lock-In Complicates Moving to Other CSPs
3. Increased Complexity that Strains IT Staff
4. Insider Threat
5. Data Loss
6. Compromised Supply Chain
7. Insufficient Due Diligence Increases Cybersecurity Risk

Set of Best Practices When Using Cloud Services

Carnegie Mellon University
Software Engineering Institute

Four Important Practice Areas

1. Perform Due Diligence
2. Managing Access
3. Protect Data
4. Monitor and Defend

Perform Due Diligence

1. Planning

- Apply (1) security architecture and design, (2) security engineering, (3) sercure coding, (4) security policy, (5) governance, and (6) risk management.

2. Development and Deployment

- Train your staff to support hybrid cloud implementations.

3. Operation

4. Decommissioning

5. Develop a multiple CSP strategy

Managing Access

1. Identify and Authenticate Users

- Accept ultimate responsibility for identity and access management (IAM), configuration management, monitoring and log analysis, and data security.

2. Assign User Access Rights

3. Create and Enforce Resource Access Policies

Protect Data

1. Protect Data from Unauthorized Access
2. Ensure Availability of Critical Data
3. Prevent Disclosure of Deleted Data

Monitor and Defend

1. Monitor Cloud-Deployed Resources
2. Analyze Both Cloud and On-Premise Monitoring
3. Coordinate with the CSP

Approach to Assess the Risk of Transitioning to Cloud Services

Carnegie Mellon University
Software Engineering Institute

Mission Risk Diagnostic Cloud Adoption Risk Factors

Carnegie Mellon University Software Engineering Institute

Risk Factors for Planning and Preparation	MRD Question
1. Business Case	Does the organization's business case justify the decision to move to the cloud?
2. Strategy	Does the organization's cloud strategy sufficiently define the role of cloud computing in the organization?
3. Plan	Is the plan for adopting and maintaining cloud technologies sufficient?

Risk Factors for Governance and Management	MRD Question
4. Governance	Are the organization's governance practices sufficient for managing cloud services?
5. Financial Management	Are the organization's financial processes sufficient for managing cloud services?
6. Change Management	Has the organization implemented an organizational change management plan for the cloud initiative?
7. Supplier Management	Does the organization have a systematic process for evaluating, selecting, and managing cloud service providers (CSPs)?

Mission Risk Diagnostic Cloud Adoption Risk Factors

Carnegie Mellon University Software Engineering Institute

Risk Factors for Organizational Capability	MRD Question
8. Organizational Roles and Responsibilities	Has the organization staffed a core team for adopting cloud technologies?
9. Organizational Competencies	Do people working on the cloud adoption initiative have the knowledge, skills, and abilities they need to do their jobs?
10. Task Execution	Are the cloud adoption initiative's tasks being performed effectively and efficiently?
11. Coordination	Are cloud adoption and implementation activities within each team and across teams coordinated appropriately?
12. Tools and Technology	Are cloud team member familiar with and able to use each CSP's native tools?
13. Resilience	Does the cloud initiative have sufficient capacity and capability to manage unexpected events and changing circumstances?

Risk Factors for Environment	MRD Question
14. Organizational Conditions	Are enterprise, organizational, and political conditions facilitating execution of the cloud initiative?
15. Compliance	Do cloud services comply with applicable laws, regulations, and mandates?

Mission Risk Diagnostic Cloud Adoption Risk Factors

Carnegie Mellon University Software Engineering Institute

Risk Factors for Engineering Lifecycle	MRD Question
16. Requirements	Does the organization fully understand the requirements for the cloud environment?
17. Architecture	Does the enterprise architecture sufficiently mitigate risks of the public cloud?
18. Implementation and Integration	Is each CSP's platform well integrated with critical core infrastructure services that reside on-premises?
19. Test and Evaluation	Are test-and-evaluation (T&E) processes, methods, and tools for the cloud environment sufficient?
20. Operations	Are processes for operating and maintaining the cloud environment sufficient?

Risk Factors for Quality-of-Service	MRD Question
21. Performance	Will cloud services meet the organization's performance requirements?
22. Agility	Will cloud services be sufficiently agile to meet the organization's business requirements?
23. Availability	Will cloud services meet the organization's availability requirements?
24. Security	Will the cloud environment be acceptably secure?

Additional Information

https://insights.sei.cmu.edu/blog/12-risks-threats-vulnerabilities-in-moving-to-the-cloud/

https://insights.sei.cmu.edu/blog/best-practices-for-cloud-security/

https://insights.sei.cmu.edu/blog/a-method-for-assessing-cloud-adoption-risks/

Mission Risk Diagnostic (MRD) Method Description

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=10075

Security Engineering Risk Analysis (SERA) Collection

https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=485410