NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER

ENTERPRISE THREAT BULLETIN


*This Bulletin is from NCSC's Enterprise Threat-Mitigation Directorate (ETD) and the National Insider Threat Task Force (NITTF)*

# Cloud Computing: Risk Considerations

## ETD Bulletin 2024-012; May 2024

Cloud computing has revolutionized the way government and private sector organizations access, manage, and store data. The migration to cloud technology offers faster innovation, flexible resources, and economies of scale. On the other hand, cloud platforms also present organizations with risk complexities that should be considered from **insider threat and Operations Security (OPSEC) perspectives**. Whether operating in a traditional, physical computing infrastructure, or in a cloud-based virtual environment, a malicious insider has the capacity to misuse their access, compromise data integrity, and exfiltrate sensitive information.

This bulletin lists some planning recommendations and best practices for security and risk mitigation components as they support their organization's Chief Information Officers (CIOs) and other mission owners who operate in diverse cloud environments:

- Conduct a comprehensive **risk assessment** of cloud service provider(s), data center owners/operators, and any other third parties who may have some level of connection to your data. A compendium of your most sensitive information (crown jewels) and who can access it should be part of this assessment.
- Ensure User Activity Monitoring **(UAM)** and Data Loss Prevention (**DLP**) capabilities are deployed and configured to monitor user "endpoints" to enhance the detection and attribution of suspicious activity.
- Coordinate with data managers to maximize **enterprise audit** collection and access to help insider threat programs detect anomalous activity and conduct investigative/damage assessment activities in response to an unauthorized disclosure.
- Collaborate with your Chief Information Security Officer (CISO) and CIO to implement strict technical **security controls** and processes to remediate misconfigurations and vulnerabilities.
- Introduce further levels of monitoring and oversight of your cloud environment's **privileged users**.
- Help implement your organization's **Zero Trust Architecture,** since it discourages or prevents an insider from accessing information they are not authorized to handle through continuous verification of identity and strict access control.
- Integrate cloud computing into your **insider threat and OPSEC strategies** and awareness campaigns.

**Safeguarding data security protocols is critical and the responsibility of all information technology users! Remember to engage with your CIO continuously!**

For additional information on Insider Threats, please visit the NCSC website.