DRAFT

Cloud Computing Security Impediments and Mitigations List

v06

July 13, 2011

Table of Contents

1. Overview 1
2. <impediment-name> *(as short as possible while being descriptive)* 2
3. Process Oriented 3
   - 3.1 Confusion about Application of 800-53-style Controls, and Compliance 3
   - 3.2 Lack of Cloud Audit Assurance and Log Sensitivity Management 3
   - 3.3 Need Clear Certification and Accreditation Guidelines 5
   - 3.4 Need Clear E-discovery Guidelines 5
   - 3.5 Need Clear Privacy Guidelines 7
   - 3.6 Need Clarity on Security Control Roles and Responsibilities 7
   - 3.7 Need to Assess Trustworthiness of Cloud Operators 9
   - 3.8 Business continuity and disaster recovery 9
4. Focused Technical 11
   - 4.1 Lack of visibility for customers 11
   - 4.2 Lack of control for customers 12
   - 4.3 Limited Data Protection 13
   - 4.4 Risk of Account Hijack 14
   - 4.5 Identity and Access Management (IAM) and Authorization not Deployed 15
   - 4.6 Risk from Multi-tenancy 15
   - 4.7 Cloud Based Denial of Service 17
5. References 19

Disclaimer: Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by the National Institute of Standards and Technology, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

1. Overview

This working document records a list of security issues that appear to be obstacles to the adoption of cloud computing by Federal agencies, and possible mitigations. The issues listed here have been added by members of the NIST security working group, or by NIST, and do not necessarily represent consensus by the group. The working group's charter and meeting notes can be found at: http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/CloudSecurity.[1]

Goal of the Security Working Group: Mitigate security impediments that may prevent adoption of cloud computing by Federal agencies.

[1] The online charter is being updated for consistency with this document.

Main Deliverable of the Security Working Group: A mature version of this working document, the "Cloud Computing Security Impediments and Mitigations List". The working group and NIST will expand this document to contain a prioritized list of security impediments and, for each impediment, either a pointer to work that mitigates the impediment, or a description of approaches for mitigation.

Schedule:

June 15, 2011 - first draft
subsequent versions approximately every 2 weeks as appropriate
Sep. 30, 2011 - final draft

Approach: The WG nominates impediments and mitigations as necessary, critiques existing impediments and mitigations, and provides rationale for each. NIST maintains and guides the writing of the impediments list. The next section provides a **template** for expressing an impediment and its associated mitigations. The purpose of this template is to help communicate impediments and related mitigations quickly without a lot of effort on the format itself, but with enough structure to remind authors of key aspects. Draft or incomplete impediment sections are expected: this is a working document.

Subsequent sections document security impediments that have been captured from feedback on the cc_security@nist.gov email list and through discussions with the working group. They are divided into two groups: process oriented and focused technical.

2. <impediment-name> *(as short as possible while being descriptive)*

Description: *A paragraph-sized (or less) description of the impediment.*

Importance: *A sentence or paragraph-sized rationale for why we should care: why does this impediment matter?*

Solution Maturity: *An informal English-language summary of how close current techniques are to mitigating the impediment, and an estimate of how feasible mitigation is in the 12-month timeframe.*

Mitigation 1: <mitigaton-name>

Text here should describe a mitigation of the impediment and how sufficient the mitigation is. The first part should take one of two forms:

1. *The text can be an English-language narrative of how to mitigate the impediment. This narrative might be similar in form to the text in a success scenario for a NIST SAJACC technical use case. E.g., see: http://collaborate.nist.gov/twiki-cloud-computing/bin/view/CloudComputing/UseCaseOpenAccount .*

OR

2. *The text can be a short synopsis of what others have done for this mitigation (perhaps a paragraph), along with a URL pointing to their public work. If the document identified is large, the text should include some navigation information, like page numbers or section names to help the reader quickly find the relevant material.*

Sufficiency Comment: *Informally characterize the effectiveness of this mitigation, and whether it depends on any other mitigations.*

Mitigation 2: ...

...

Mitigation *n*: ...

Active WG Members: *Names of WG members who are helping with this impediment and who wish to be identified.*

References: *We anticipate that different mitigations will share references, so this field will ultimately exist at the end of the document in its own section but may initially exist per-section.*

3. Process Oriented

The process-oriented issues rely on human-centered processes, procedures, and guidance for mitigation.

3.1 Confusion about Application of 800-53-style Controls, and Compliance

Description: Need for clarity on how 800-53-style control guides can work for the cloud.

Importance: TBD.

Solution Maturity: TBD.

Mitigation 1: FedRAMP

A list of security controls for a cloud system, with details similar to 800-53...

Sufficiency Comment: TBD.

Active WG Members: Michael Berman, others TBD.

References: TBD, but clearly including the FedRAMP document URLs.

3.2 Lack of Cloud Audit Assurance and Log Sensitivity Management

Description: How to gain assurance that:

1. Important events are monitored, and
2. Sensitive/private audit logs are appropriately protected, and
3. Integrity of audit data used for initial or continuous auditing purposes e.g. audit logs; data collected by Security Content Automation Protocol (SCAP) etc.
4. Audit data interchange incompatibility.

Importance: TBD.

Solution Maturity: TBD.

Mitigation 1: Risk management framework

The NIST Risk Management Framework (SP800-37) provides guidance to federal system owners to take a risk-based approach to securing systems. This approach is operationally focused and is intended to facilitate the monitoring, documenting, and mitigation of threats on a regular if not near real time basis. Continuous monitoring is step 6 of SP800-37's 6-step risk management framework. While many vendors are seeking to offer automated vulnerability monitoring tools, it is important to realize that there is more to an effective continuous monitoring program than the automated tools. The FedRAMP program's Proposed Security Assessment and Authorization document (https://info.apps.gov/sites/default/files/Proposed-Security-Assessment-and-Authorization-for-Cloud-Computing.pdf) describes an effective continuous monitoring program as one that includes:

- "Configuration management and control processes for information systems;
- Security impact analyses on proposed or actual changes to information systems and environments of operation;

- Assessment of selected security controls (including system-specific, hybrid, and common controls) based on the defined continuous monitoring strategy;
- Security status reporting to appropriate officials; and
- Active involvement by authorizing officials in the ongoing management of information system-related security risks."

Sufficiency Comment: TBD.

Mitigation 2: Data Integrity Protection

"To support consistent, well-informed, and ongoing security authorization decisions (though continuous monitoring), transparency of security and risk management-related information and reciprocity" (NIST 800-37) trustworthy audit data needs to be available upon request.

Throughout the audit data´s lifecycle it needs to be:
In transit

- Encrypt data using a one-time session key similar to how SSL/TLS works.

In Storage

- Preserved in accordance to records management standards e.g. National Archives and Records Administration (NARA) statues, including the Federal Records Act (44 U.S.C. Chapters 21, 29, 31, 33) and NARA regulations (Title 36 of the Code of Federal Regulations, Chapter XII, Subchapter B) etc.
- "The information system protects audit information and audit tools from unauthorized access, modification, and deletion" (NIST SP 800-53 AU-9)
- The audit information´s integrity shall be protected within a timely manner. " System logs need to be protected, because if the data can be modified or data in them deleted, their existence may create a false sense of security". (ISO27002)
- Audit data may be needed for evidentiary purposes which would require its evidential weight and chain of custody to be preserved to ensure it is admissible. See US Federal Rules of Evidence; BS 10008 Evidential weight and legal admissibility of electronically stored information
- Where the technical solutions involve cryptography, FIPS 140-2 is applicable

Sufficiency Comment: TBD.

Mitigation 3: Audit Data Interchange

- The Cybersecurity Information Exchange Techniques (CYBEX) project was launched by the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T). Cybex provides for the structured exchange at known assurance levels of information about the measureable "security state" of systems and devices, about vulnerabilities, about incidents such as cyber attacks, and about related knowledge "heuristics." The CYBEX initiative imports more than twenty "best of breed" standards for platforms developed over the past several years by government agencies and industry to enhance cyber security and infrastructure protection. Pulling these platforms together in a coherent way to provides for:
    - "locking down" on-line systems to minimize vulnerabilities
    - capturing incident information for subsequent analysis when harmful incidents occur
    - discovering and exchanging related information with some degree of assurance

  The CYBEX Model includes:
    - structuring cyber security information for exchange purposes
    - identifying and discovering cyber security information and entities
    - establishment of trust and policy agreement between exchanging entities
    - requesting and responding with cyber security

  - assuring the integrity of the cyber security information exchange
- TBD – see Cloud Trust Protocol

Active WG Members: Nadeem Bukhari, Fred Whiteside, others TBD.

References:

- CSA Cloud Audit - http://cloudaudit.org/page5/page5.html
- CSA/ CSC - Cloud Trust Protocol - http://assets1.csc.com/lef/downloads/Digital_Trust_in_the_Cloud.pdf
- The FedRAMP document: https://info.apps.gov/sites/default/files/Proposed-Security-Assessment-and-Authorization-for-Cloud-Computing.pdf
- NIST 800-53 AU9 – Protection of audit Information
- PCI DSS 10.5.5 – File Integrity Monitoring
- ISO27001 10.10.3 – Protection of Log Information
- NIST SP 800-92
- CSA CCM SA-14 – Audit Logging / Intrusion Detection
- CYBEX Overview - http://www.itu.int/dms_pub/itu-t/oth/0A/0D/T0A0D00001D0004PDFE.pdf

3.3 Need Clear Certification and Accreditation Guidelines

Description: How to certify and accredit cloud solutions with confidence.

Importance: Executive departments and agencies, in effectively managing information security risks inherent in all modern computing technologies, must have a high degree of trust and confidence in the entities providing new and innovative technologies, including cloud technologies and services.

Solution Maturity: Pending approval of OMB memo formalizing FedRAMP Program.

Mitigation 1: The FedRAMP will provide a cost-effective, risk-based approach for the adoption and use of cloud services. Establishing clear and concise expectations for security and privacy based on current threats, taking advantage of innovative, open, and state-of-the-practice solutions for the protection of Federal information in cloud-based information systems, and ensuring a high degree of transparency in security and privacy solutions, will promote a climate of trust between consumers and providers of cloud services. http://www.fedramp.gov

Sufficiency Comment:

Active WG Members: Lisa Carnahan, others TBD.

References:

- http://www.fedramp.gov
- Note to editor: include standard REFERENCE 800-53 and 800-53A.

3.4 Need Clear E-discovery Guidelines

Description:

1. How to provide access to data in response to lawful authority while protecting customer privacy.
2. How to ensure service providers are preserving electronic records with sufficient evidential weight and chain of custody controls

Importance: Meeting electronic discovery requests can pose a significant challenge when electronically stored information (ESI) is in the cloud.

Customer:

The cloud customer is responsible for preserving evidence and issuance of litigation hold notices to cloud providers who have any pertinent ESI. If required evidence is lost or damaged, the customer may be fined and/or sanctioned by the court despite any fault or failure on the part of the cloud provider, thus it is incumbent upon the cloud customer to verify that robust processes are in place to ensure preservation and facilitate ESI collection. Additionally, failure to understand where pertinent ESI is located could result in exposure of data beyond the scope of the electronic discovery request, or data belonging to customers who are not parties to the specific discovery request – possibly violating their privacy.

Provider:

The cloud provider is responsible for providing information to lawful authority when presented with a lawful demand for such information. This may be a one-time request for stored information or it may be a request for dynamic access to data akin to a wiretap. These requests often include a specific deadline for cooperation or surrendering of the information and the provider may face penalties if they are unable or unwilling to comply.

Solution Maturity: Involving legal/E-discovery SMEs in cloud service negotiation and mapping of business processes to identify points where ESI is generated, processed, and/or stored on cloud based systems are solutions which can be implemented immediately and offer reasonable mitigation of risk. Automation of ESI collection and preservation management is potentially a future mitigation, but limitations of current tools and evolving nature of the cloud environments can result in the required interaction between the two providing a less than optimal solution at present.

Mitigation 1: When procuring a cloud service, customers must gain an understanding of how the cloud provider processes electronic discovery and litigation holds. The customer should acquire knowledge of key issues – such as the length of time the provider takes to enforce a litigation hold (i.e. prevent the modification and/or destruction of pertinent evidence) or respond to an electronic discovery request and what steps are required to invoke these processes, types of logs and metadata retained including lifecycles of same, dependencies on other providers, evidentiary chain of custody and storage, and additional processing fees that may be incurred. Having a subject matter expert discuss these processes with the cloud provider is preferable to a checklist, due to the variances of cloud environments and the specialized knowledge requirements around electronic discovery and preservation of evidence. Specific wording or clauses may need to be inserted into the cloud contract to ensure that cloud providers share the burden for failure to properly secure and maintain evidence once a hold or request has been properly initiated.

Sufficiency Comment: While this solution provides a reasonable level of risk mitigation, it is dependent upon the existence and availability of in-house knowledge, or the willingness to procure such, and to invest the time and resources needed. There may also be unanticipated requests for specific metadata or unstructured data not routinely collected or stored by either the cloud customer or provider that limit the availability of same and these must be handled on a case by case basis.

Mitigation 2: Customers should undertake the effort to map significant business processes and ESI created, processed, and/or stored as a result that would have a high likelihood of being the target of an electronic discovery request. Where possible, the proactive collection, indexing, and storage of ESI that has a reasonable expectancy of falling within the scope of future litigation or discovery requests (such as email) may lessen the dependency on cloud providers – particularly if the ESI can be stored on systems under the direct control of the customer. A records retention

policy defining the forms of ESI routinely collected and archived, as well as ESI formats not retained, can assist in refining the scope of this effort.

Sufficiency Comment: While this solution provides a reasonable level of risk mitigation, it is dependent upon the ability and willingness of the customer to map key business processes and the discovery-pertinent ESI generated, processed or stored as a result. There is a cost associated with mapping processes and storing ESI, and these should be balanced against costs of electronic discovery and litigation hold involving cloud providers, costs of hiring E-discovery specialists to handle ESI projects, and the possibility of fines and/or sanctions as the result of an inability to preserve or produce requested evidence.

Mitigation 3: Providers should undertake the effort to understand the requirements for lawful intercept, National Security Letters, Subpoena, and e-Discovery. Providers must make a timely response and provide information for a specific tenant without collateral information from other tenants. Providers must be able to locate and provide access to data or communication channels that are specific to a single tenant.

Sufficiency Comment: Existing hypervisor platform technologies do not incorporate the necessary features to support these tasks. Providers will need to incorporate in-house or 3rd party solutions.

Active WG Members: Michael Berman, Nadeem Bukhari, Ken Stavinoha, others TBD.

References:

- Federal Rules of Civil Procedure (2010).

3.5 Need Clear Privacy Guidelines

Description: How to build confidence that cloud solutions provide privacy.

Importance: TBD.

Solution Maturity: TBD.

Mitigation 1: TBD.

Sufficiency Comment: TBD.

Active WG Members: Michele Drgon, others TBD.

References: TBD.

3.6 Need Clarity on Security Control Roles and Responsibilities

Description: Who (among cloud actors such as customer and provider) should be responsible for the implementation of required security controls listed in section 1.1? It seems that the actor most able to observe and configure specific a portion of a cloud implementation would be in the best place to implement a relevant control.

Importance: The data owner (typically cloud customer) is responsible for compliance with laws and regulations including the proper security controls around their data, regardless of its location or the involvement of other parties.

Customer:

When customer data is off-premise and under the control of a third party (such as the cloud provider, cloud broker, or cloud carrier), the ability of the data owner to implement security controls is often limited. In cloud computing environments, the implementation of controls is

going to be largely dependent upon the type of service (IAAS, PAAS, SAAS), type of cloud (Private, Public, Community, Hybrid) type of control (i.e. physical versus logical) and the specifications of responsibility delineated in the cloud contract. Customers must choose services accordingly and understand the risks and limitations of third party control – i.e. customers can outsource the functionality of a role/responsibility, but will still hold the legal liability for failure to secure data.

Provider/Broker/Carrier:

Cloud providers/brokers/carriers have increasing responsibilities for implementing and maintaining security depending on the cloud types and service types offered. For example, physical security controls in the cloud environment will have to be implemented by a party which has access to the physical property where the assets reside – a role likely performed by the cloud provider, broker, or carrier. Providers/brokers/carriers should provide statements of the security controls environment implemented and maintained by them for each of the cloud architectures and services offered.

Solution Maturity: Cloud Security Alliance has published a Cloud Controls Matrix which provides a good reference point and denotes applicability to cloud service type (IAAS, PAAS, SAAS) and scope (provider, tenant). The solution effectiveness is dependent upon the cloud customer's willingness to understand the provider posture on security controls for the services offered and the ability of potential providers to mitigate specific risks and meet customer requirements. The solution may also be dependent upon customer willingness to choose a cloud service or architecture (plus availability of same) that permits more direct control to address specific security requirements.

Mitigation 1: Provider-subscriber guidelines.

Document roles and responsibilities definitions or guidelines for cloud provider and consumer/subscriber. Clarity about how responsibility for protection of information remains with a system owner but the terms of a contract between a system owner and a cloud provider can place an obligation on the provider to protect information. To satisfy due diligence and due care requirements for securing their data, cloud customers must ensure the contract with the cloud provider/broker/carrier specifies the responsible party (or parties) for implementing and maintaining security controls and provides rights of action for failure to implement or maintain same.

Sufficiency Comment: The solution provides a reasonable degree of risk mitigation but is dependent upon customer willingness to define security roles/responsibilities and negotiate same with the cloud provider(s).

Mitigation 2: Cloud type/service selection.

In cases where a larger degree of direct control over security roles/responsibilities and the ability to implement security controls is needed, cloud customers may consider utilization of a type of service (i.e. PAAS, or IAAS instead of SAAS) and/or a cloud type (on-premise versus off-premise, private versus public cloud) which will allow that requirement to be fulfilled.

Sufficiency Comment: The solution can provide reasonable degree of risk mitigation but there may be increased cost in choosing services and/or architectures that allow more direct control and these costs should be weighed against security requirements and acceptable risk levels.

Active WG Members: Ken Stavinoha, others TBD.

References:

- CSA Cloud Controls Matrix.

3.7 Need to Assess Trustworthiness of Cloud Operators

Description: Not being able to fully trust cloud operators is one of the primary reasons for the reluctance to adopt cloud services and solutions. Despite this, cloud operators are still hesitant to divulge all their security practices in fear of giving away intellectual property. This is problematic for cloud service consumers that have invested significant amount of resources over the past several years (with Sarbanes-Oxley, FISMA, etc.) gaining transparency into their own IT infrastructure. The ability for consumers to assess cloud operators is vital for the secure adoption of cloud computing.

Importance: For cloud service consumers, it is critical to know the security practices of their cloud operators in order to maintain and improve on the security of their data and their IT environment. This means that cloud consumers need to know what their cloud operators are doing and if their cloud operators are effectively performing those functions. In addition, cloud consumers must be able to randomly and independently verify their cloud operators' practices.

Solution Maturity: The practices and technology currently exist to address this impediment. Security control frameworks exist (such as CoBIT, ISO 27000, NIST SP 800-53, etc.) in order to architect and assess the security posture of an organization. NIST-validated SCAP-compliant tools exist to identify and verify vulnerability and configuration data, and virtualization management modules also exist to provide additional insight into the virtual infrastructure. The shift that may need to occur is tailoring the frameworks and the technology for the cloud and a cultural shift to provide the needed transparency.

Mitigation 1: cloud provider human resources practices

Provider staff screening, hiring, training, monitoring, separation of duty, malicious insider.

Sufficiency Comment: TBD.

Active WG Members: Carlo Espiritu, others TBD.

References: TBD.

3.8 Business continuity and disaster recovery

Description: Even in traditional IT operations, business continuity planning (more specifically, contingency planning) is complex, and the effectiveness of its implementation is difficult to test and verify. More often than not, when disasters occur, unexpected disruptions create confusion and result in less efficient recovery practices. Cloud computing adds more complexity to IT infrastructure and obfuscates responsibility between cloud provider and customer. There is an elevated concern of business continuity and disaster recovery in this new paradigm.

Importance: As pointed out in section 4.8 Availability, NIST SP 800-144, outages due to high level disruptions do occur in cloud computing services despite redundant architectures designed for high availability. In addition, the value concentration in clouds makes them the preferred targets of malicious attacks. Consequently, it is important to plan and implement business continuity and disaster recovery in consideration of the characteristics of cloud computing:

- The intricate business relationship and managerial responsibility (ownership and governance) in cloud computing complicate business continuity planning and implementation and effective disaster recovery.
- The large scale, complexity and dynamics of cloud infrastructure make it even more difficult for maintaining business continuity and performing disaster recovery.

- Comingled data and services result in comingled responsibilities and contingency plans.
- Clustering, quick provisioning and on-demand self-service provide conduits for disruptions to propagate through the cloud environment.
- However, economies of scale in cloud computing have the potential to provide a full range of backup sites and to carry out effective testing and exercises in order to validate security controls of contingency planning.

Solution Maturity: Documented security policies and procedures, clustering technologies, alternate sites and backup have all been used in traditional IT contingency planning and implementation. How effective they are in cloud computing (with order of magnitude increase in scale, complexity and dynamics) remains to be seen. Clear roles and responsibilities and close collaboration between cloud provider and customer are necessary for any effective business continuity and disaster recovery. It is also necessary to coordinate incident response activities with contingency planning activities between cloud provider and customer.

Mitigation 1: Consistent policies and procedures

- Develop a contingency plan for a cloud-based application or system using guidelines in NIST SP 800-34 Rev 1 and in Domain 9: Contingency Planning, Federal Cloud Security Guidelines (if published).
    - Determine ownership, data sensitivity, cloud service and deployment models, roles and responsibilities.
    - Set recovery priorities and map resource requirements accordingly.
    - Provide a road map of actions for activation, notification, recovery procedures, and reconstitution.
    - Enforce policies and procedures through SLAs.
- Incorporate customer' contingency plan for individual application and/or system into cloud provider's overall contingency plan.
- Establish management succession and escalation procedures between cloud provider and customer.
- Reduce the complexity of the recovery effort.

Sufficiency Comment: To be effective, this mitigation needs unprecedented close collaboration between cloud provider and customer and among customers. Since recovery priorities are based on mission requirements and data sensitivity, applications should be partitioned according to sensitivity as suggested in mitigations of multi-tenancy.

Mitigation 2: Clustering and redundancy

- Shared storage clusters.
- Hardware level clustering.
- VM clusters.
- Software clustering (application servers and database management systems).

Sufficiency Comment: The key to clustering security is isolation (logical separation), and its sufficiency is addressed in the mitigations of multi-tenancy.

Mitigation 3: Alternate sites and backup

- NIST SP 800-53 Rev3 recommends:
    - Alternate storage and processing sites.
    - Alternate telecommunication services.
    - Information system backup.
- Provide cold, warm and hot backup sites (economies of scale).

- Outsource information system backup to a cloud backup service.
- Use multiple cloud providers.
- Supplement cloud provider's backup schemes with customer's non-cloud sites.

Sufficiency Comment: A hot backup is a preferred solution to down time for high available systems, but may not be included in providers' basic services and is expensive compared to alternatives.

Mitigation 4: Effective testing and exercises

- Test the contingency plan periodically to verify its effectiveness (including personnel training) and if it's updated to reflect recent changes.
- Perform contingency plan testing and exercises against high level disruptions to discover deep-rooted risks.
- Provide production-like testing environments for contingency plan testing and exercises.

Sufficiency Comment: Agencies are constrained to simulate level 3 and 4 disruptions in their core production environments. And there are resource limitations to provide production-like testing environments. As a result, contingency plan testing and exercises are usually tabletop scenario exercises or at best consist of some failovers in peripheral equipments.

Active WG Members: Shilong Chu, others TBD.

References:

- NIST SP 800-34 Rev 1
- NIST SP 800-53 Rev 3
- NIST SP 800-144
- Federal Cloud Security Guidelines (2011)

4. Focused Technical

The focused technical issues are amenable to automated mitigation mechanisms.

4.1 Lack of Visibility for Customers

Description:

- How can cloud subscribers (customers) observe their workloads to be aware of their security, compliance, privacy, health and general status?
- And how can subscribers instruct the cloud as to what kind of information they are interested in?
- Today, subscribers have very limited visibility into incident/alert and audit information generated by the cloud provider related to the subscriber's activities on the cloud. Most of this information is used internally by the provider
- Available tools are piecemeal and specific to each provider, which renders a multi-cloud mashup unmanageable

Importance:

- Cloud subscribers are ultimately liable for security, compliance, privacy: Security/compliance/privacy regulations specifically state that ultimate liability cannot be outsourced, and providers do not take on full responsibility for this in their SLAs
- Cloud subscribers are ultimately liable for most health and general status. Providers usually compensate for the subscription cost of an outage, but not for the actual damage or loss of business caused

Solution Maturity:

- Some standards are emerging that let subscribers instruct the cloud as to what kind of information they are interested in (e.g. CloudAudit)
- Standards are maturing for alert exchange.

Mitigation 1: Audits

- CloudAudit.org is a Cloud Security Alliance standardization initiative that allows subscribers to tell providers what information they require and in what format. The maturity seems to be relatively immature at this stage (unclear whether there are actual implementations yet), but it is moving forward

  Sufficiency Comment: Once fully standardized and broadly implemented, this may be sufficient. But sufficiency depends very much on what kinds of audit monitoring the provider will support

Mitigation 2: Monitoring

- SCAP is an alert format standard mandated by US government that can help providers push alerts to subscribers in a standard format

  Sufficiency Comment: Once fully standardized and broadly implemented, this may be sufficient. But sufficiency depends very much on what kinds of audit monitoring the provider will support

Active WG Members: Ulrich Lang, others TBD.

References:

- www.cloudaudit.org
- scap.nist.gov

4.2 Lack of Control for Customers

Description:

- How can cloud subscribers (customers) maintain effective control their workloads even though the protection mechanisms and even locations of workloads may not be known to customers?
- And how can subscribers instruct the cloud as to what kind of policies they want enforced?
- Today, subscribers have very limited control over the policies enforced by the cloud provider on their behalf. Most controls are on the network layer (e.g. virtual firewalls) or the VM layer
- Today there is very little automation available to help subscribers implement technical control (policy) across their cloud applications
- Platform as a service (web service platforms) will need application layer policy enforcement

Importance:

- Much of the policy that has to be enforced is the specific policy of the subscriber, not the provider. In other words, the policy depends on the specifics of the subscriber business, business processes, regulations, policies etc.
- Providers cannot independently know and enforce those policy requirements for subscribers because subscriber policy requirements are subscriber specific
- Subscribers have no/few tools available to specify policy in their terms, and feed them into the cloud for control enforcement.
- Available tools are piecemeal and specific to each provider, which renders a multi-cloud mashup unmanageable

Solution Maturity:

- Some authorization management standards are available that could help solve this problem. E.g. OASIS XACML is at an early-stage maturity level, but not yet widely implemented/deployed.

XACML is a very technical format that makes it hard/impossible for subscribers to specify their policy requirements

- Some technologies are available that are easier for subscribers to specify their requirements and that provide a degree of automation (by reusing information from cloud mashup tools), but these not yet standardized or widely deployed, e.g. model-driven security.
- Virtual network layer policy enforcement is available in some cloud platforms, e.g. virtual firewalls. However, many of those only support proprietary policy rule formats
- Some virtual machine layer policy enforcement tools are available in some cloud platforms. However, many of those only support proprietary policy rule formats

Mitigation 1:

- Authorization management provides a standardized way to feed technical policy requirements into the cloud stack for technical enforcement
- Note: Continuous monitoring is *not* a solution here, as it does not prevent/control

Sufficiency Comment: Authorization management typically only covers the middleware layer, which the virtual network layer and virtual machine layer tools only cover their respective layer. A more joint-up enforcement stack is required to be fully effective

Mitigation 2:

- Virtual network layer firewalls can be configured for network layer firewall rule enforcement
- Note: Continuous monitoring is *not* a solution here, as it does not prevent/control

Sufficiency Comment: Only covers the network layer. Again, a more joint-up enforcement stack is required to be fully effective

Mitigation 3:

- Virtual machine layer security tools can be configured for VM layer rule enforcement
- Note: Continuous monitoring is *not* a solution here, as it does not prevent/control

Sufficiency Comment: Only covers the VM layer. Again, a more joint-up enforcement stack is required to be fully effective

Active WG Members: Ulrich Lang, others TBD.

References:

- www.modeldrivensecurity.org
- www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

4.3 Limited Data Protection

Description: data protection (move in/out of cloud, assured deletion, loss/leakage, location).

Importance: TBD.

Solution Maturity: TBD.

Mitigation 1: encryption, etc.

TBD. encrypt data wherever practical; replication; off-cloud backup; disaster recovery.

Sufficiency Comment: TBD.

Active WG Members: Michael Berman, Nadeem Bukhari, others TBD.

References: TBD.

4.4 Risk of Account Hijack

Description: Benefits of cloud computing include its easy accessibility. A customer can use cloud computing services anywhere he/she has Internet access. However, the Internet is full of threats such as phishing, pharming and spyware, whose purpose is to steal usernames and passwords (credentials). Facing this Internet security threat environment, customers adopting cloud computing are concerned about how user accounts are protected from hijack to avoid misuse.

Importance: Account hijacking is not new, but its potential is heightened in the context of cloud computing because:

- There is additional attack surface exposure due to increased complexity and dynamics in the infrastructure.
- There are new APIs/interfaces that are less battle-tested.
- A hijacked account may be used to steal information, manipulate data, and defraud others under the customer's identity.
- A hijacked account may be used to attack other tenants as an insider in the multi-tenancy environment.

Solution Maturity: Mitigations such as strong authentication, encrypted credentials, and secure APIs/interfaces have been used to protect user accounts from hijack. But, as pointed out in the Symantec Security Threat Report, the easiest vulnerability for attackers to exploit is our trust of friends and colleagues. Users tend to click the links and attachments in an email they received from a trusted source (perceived or real). Thus, these mitigations should complement effective user training and proactive monitoring and auditing of unauthorized activities.

Mitigation 1: Strong authentication

- Enforce strong password usage and change passwords periodically.
- Use multi-factor authentication.
- Prompt users for their passwords during sessions especially when there are suspicious events.
- Allow logins coming only from a white listed address range.
- Use biometrics.

Sufficiency Comment: There is already a password proliferation, resulting in security compromising behavior and increased burden on help desk. Possible considerations in cloud computing include integration with customers' exiting identity management processes and single sign-on (SSO).

Mitigation 2: Encrypted Credentials

- Provide a dedicated VPN.
- Use HTTPS and LDAPS.
- Enable secure cookies.
- Use strong cryptographic PKI keys.

Sufficiency Comment: The effectiveness of encrypted credentials depends largely on secure key management.

Mitigation 3: Secure APIs/interfaces

- Provide common security models for cloud APIs/interfaces (e.g., WS*, WS-I, SAML for web services).
- Protect application security using secure APIs/interfaces (e.g., input validation/escaping/encoding against injection exploits such as SQL injection and cross site scripting).

Sufficiency Comment: Cloud APIs/interfaces are still evolving (all the way up to the level of cloud federation).

Active WG Members: Shilong Chu, others TBD.

References: [09].

4.5 Identity and Access Management (IAM) and Authorization not Deployed

Description: How to manage identity management for federal cloud based authentication and authorization.

Importance: High.

Solution Maturity: Immature.

Mitigation 1: USG must develop a federated IAM solution for federal cloud based services. The solution will have to be developed in phases due to a lack of standard approach. The objective or end state is a single signon solution (SSO) for the entire USG to access and authorize federal cloud based services. The SAJACC NIST cloud computing use cases are being developed for the following scenarios:

5.1 Identity Management - User Account Provisioning
5.2 Identity Management - User Authentication in the Cloud
5.3 Identity Management - Data Access Authorization Policy Management in the Cloud
5.4 Identity Management - User Credential Synchronization between Enterprises and the Cloud

DHS top security controls include the following controls for IAM:

FISMA Control	Control Name
AC - 02	Account Management
AC - 03	Account Enforcement
AC - 06	Least Privilege
CM - 07	Least Functionality
IA - 02	Identification & Authentication Organizational Users
IA - 05	Authenticator Management
IA - 08	Identification & Authentication non - organizational users

Sufficiency Comment: No solution identified for USG today.

Active WG Members: Bill Butler, others TBD.

References:

- DHS Top Security Controls
- SAJACC Identity in the Cloud - Use Cases Version 1.0 OASIS
- SAJACC NIST Cloud Computing Use Cases
- Electronic Authentication Guideline. NIST Special Publication 800-63 Version 1.0.2

4.6 Risk from Multi-tenancy

Description: Cloud computing provides the potential of cost saving through resource sharing. Different tenants use services on the same cloud simultaneously. As a result, there are warranted security concerns:

1. A tenant may have access to other tenants' virtual machines, network traffic, actual/residual data, etc.

2. A tenant may impact the normal operation of other tenants, steal their data, steal their identities, etc.

Importance: Although many network services and programs have simultaneously supported multiple tenants in the past, cloud computing elevates this concern because the resource sharing is pervasive, exposes many possibly-vulnerable interfaces, and potentially occurs at a very large scale. Thus, this is a new challenge and Federal agencies are not familiar with this kind of massive resource sharing and its security ramifications. The uncertainty may impede the adoption of cloud computing. The following mitigations address these concerns by ascertaining application separation and data encryption in cloud computing.

Solution Maturity: Physical separation is a mature enough practice even in traditional IT environments. Despite key management limitations, data encryption has been accepted in eCommerce and Federal IT systems. Application partitioning facilitates putting critical components in more secure environments, but its assurance of security needs to be further verified. Logical separation in cloud computing remains a general concern and its maturity will be vendor dependent in the near future. Based on their maturity levels, it is suggested to use physical separation or a combination of data encryption, application partitioning and logical separation (defense in depth) to address the risk of multi-tenancy. All mitigations should complement the identity management and access control best practices.

Mitigation 1: Data encryption

- Data in transit: Encrypt data using a one-time session key similar to how SSL/TLS works.
- Data at rest: Selectively encrypt sensitive data using NIST 140-2 validated algorithms.
    - Manage key separately from data with higher privileges and preferably accessible only through procedures/programs.
    - Change key periodically and data unencrypted and re-encrypted with the new key.
    - Compile and/or wrap the encryption procedure/program to hide additional data transformation or padding to make it even harder for a snooper to get the key.

Sufficiency Comment: By itself, encryption is not sufficient to mitigate the risks from multi-tenancy. Encrypted data is not as vulnerable to disclosure as plaintext data but is still vulnerable to loss and possibly corruption. Key management must be performed correctly and at scale or the cryptography does not provide value. Performance may be affected.

Mitigation 2: Application Partitioning

- Separate access control functionality from business processing functionality.
- Separate logic processing functionality from data access functionality.
- Separate user functionality from system management functionality.
- Aggregate functionalities with similar security requirements to run in the same virtual environment and take advantage of modern compartmentalized data centers (vLANs/sub-network zones with varying levels of security controls).

Sufficiency Comment: By itself, localization is not sufficient to mitigate the risks from multi-tenancy but it can localize the reach of security risks and hence reduce risks.

Mitigation 3: Logical separation

- Support holistic logical separation of the resources at all the layers: computing (virtualization), networking (vSwitches and vLANs) and storage (logical separation of files with access controls).

- Secure the virtualization server (hypervisor isolation settings to limit accesses).
- Secure the virtual network by working hand-in-hand with the physical network security, especially against man in the middle attacks (MAC spoofing and ARP poisoning).
- Harden the Virtual Machine (VM) so that the virtualization layer is not exposed to attack.

Sufficiency Comment: If logical separation is faithfully implemented, it addresses much of the multi-tenancy impediment. The difficulty is in achieving assurance that an implementation is correct.

Mitigation 4: Physical separation

- Special virtual environments with physical separation of the full-stack cloud infrastructure can be provisioned to customers with special security requirements.
- This kind of special virtual environments can be provisioned in a cookie cutter way to respond to increasing demands.

Sufficiency Comment: Consider private cloud for even higher demand for separation/isolation.

Active WG Members: Shilong Chu, Lee Badger, others TBD.

References: [01] through [08] Inserted in section 5.

4.7 Cloud Based Denial of Service

Link to 3.8 Business continuity and disaster recovery

(Cloud Consumer)

Description: Because cloud customers depend on functional networks to access their Resources, and because networks are often not under the control of customers, there is a risk that the cloud may not be reachable. **Note:** high latency on the cloud carrier network may have the same net effect as DoS.

Importance: High.

Solution Maturity: TBD.

Mitigation 1: Cloud Consumer adopts hybrid approach with Cloud Broker to contract with two or more Cloud Providers (Cloud Broker service aggregation) (NIST, p23).

Sufficiency Comment: See usage scenario one of the NIST RA (2011). An outage experienced by one Cloud Provider will not result in total loss of Cloud Consumer access to cloud based data unless Cloud Provider two experiences an outage as well.

Mitigation 2: Cloud Consumer contract Cloud Carrier (or Cloud Broker) for diverse network access from customer site(s) to the by Cloud Carrier network. Cloud Consumer site(s) access diversity can take the form of ingress/egress, route, switch, serving wire center and interconnection points (Cloud Broker service Intermediation) (NIST, p23).

Sufficiency Comment: See usage scenario one of the NIST RA (2011). Network diversity between the Cloud Consumer site(s) and Cloud Carrier points of presence is a sound strategy to address the risk of denial of service (DoS).

Mitigation 3: Cloud Consumer contract Cloud Carrier, or Cloud Broker, for redundant customer premises equipment (CPE) with failover (FO) capability to provide high availability network access to compliment diverse network access to Cloud Provider network.

Sufficiency Comment: See usage scenario one of the NIST RA (2011). The Cloud Carrier, through its transport agent for example, shall provide required equipment as part of the cloud based service contract with appropriate SLA's. The equipment SLA's include provisions such as (equipment monitoring, service, upgrades, repair, replacement and technology refresh).

CSA Cloud Control Matrix: Control Area: Operations Management - Equipment Maintenance Policies and procedures shall be established for equipment maintenance ensuring continuity and availability of operations.

MA-2 Controlled Maintenance
MA-3 Maintenance Tools
MA-4 Non-Local Maintenance
MA-5 Maintenance Personnel
MA-6 Timely Maintenance

** NIST SP 800-53 Controls

Active WG Members: Bill Butler, Mike Nelson, others TBD.

References:

- CSA Cloud Control Matrix
- Federal Risk and Authorization Management Program (FedRAMP)
- NIST Cloud Computing Reference Architecture (30 March 2011), Version 1
- NIST SP 800-53

(Cloud Provider)

Description: In spite of clauses in SLAs implying high availability and minimal downtimes for subscribers, service or utility outages are inevitable due to man-made causes (e.g., malicious attacks or inadvertent administrator errors) or natural causes (e.g., floods, tornados, etc.) (NIST 800-146, p8-3). Cloud providers depend on functional networks to provide resource access to cloud consumers, and because cloud carrier networks are often not under the control of cloud providers, there is a risk that the cloud may not be reachable or infrastructure and/or data not available or severely degraded. It is possible that the cloud based data is available but the network is not. It is possible that the cloud carrier network to be available but the cloud provider service and data are not available. Both scenarios equate to cloud service denial from the cloud consumer perspective.

Denial of service:	**Customer**	**Provider**
Network denied	DoS	
Service denied	DoS	DoS
Data denied	DoS	DoS

Importance: High.

Solution Maturity: TBD.

Mitigation 1a: (network) Cloud Provider adopts hybrid approach by contracting with two or more cloud carriers for access network to cloud consumer(s) (NIST RA, p24).

Sufficiency Comment:

Cloud provider connected to two cloud carriers, which connect to cloud consumer providing redundant paths. An outage experienced by one cloud carrier will not result in total loss of cloud provider access to cloud consumers.

Action: Create usage scenario four (NIST RA (2011) to depict 4 node topology (cloud consumer, (2) cloud carriers and cloud provider

Cloud brokers, through service aggregation or arbitrage provide diverse network for cloud provider (access, distribution and core network layers).

Mitigation 1b: (network) NIST Cloud Computing Standards Roadmap – 092 5 Jul, 2011 scenario eight discusses cloud consumer access across multiple clouds, simultaneously, as a mitigation strategy

Deployment Case 2: In the distributed deployment cases, a single cloud consumer has an application that may be distributed across two or more cloud providers and administrative domains simultaneously. While the cloud consumer may have simple consumer-provider interactions with their application and the providers, more complicated Peer-to-Peer ("P2P") interactions may be required -- between both the consumer and provider and also between the providers themselves.

Sufficiency Comment: This solution will require the development of interoperability standards and contractual relationships between cloud providers. Also more research is required into the effects of these mitigation strategies have on cloud based risk to the cloud consumer.

Mitigation 2 (service): Cloud provider must provide a highly redundant, high availability service, resource abstract and control physical resource layers (NIST , RA, p15). These three layers are all required to provide a cloud service to cloud consumers within the cloud provider boundary. Cloud provider must be required to have COOP/DR plans in place by cloud customer contract / SLA.

Sufficiency Comment: The physical building and the three layers (service, resource and physical) must be redundant, resilient, and fault resistant. NIST 800-146 (p 8- suggests the following mitigation strategies:

1. SLA Evaluation
2. Portability of Workloads
3. Interoperability between Cloud Providers
4. Disaster Recovery

Mitigation 3 (data): Cloud provider must provide redundant data instances (protect data availability) through various strategies and control measures.

Sufficiency Comment: I need help here from VM and virtual computing experts or the Data WG to characterize a survival data deployment in the cloud computing context.

Active WG Members: Bill Butler, Mike Nelson, others TBD.

References:

- NIST Cloud Computing Standards Roadmap – 092 5 Jul, 2011
- NIST Cloud Computing Reference Architecture v1. Dated 30 March, 2011
- CSA Cloud Control Matrix
- Draft Cloud Computing Synopsis and Recommendations - http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf

5. References

[01] Draft Cloud Computing Synopsis and Recommendations - http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf

[02] Proposed Security Assessment & Authorization for U.S. Government Cloud Computing - http://www.cio.gov/pages.cfm/page/Federal-Risk-and-Authorization-Management-Program-FedRAMP

[03] Security Guidance for Critical Areas of Focus in Cloud Computing V2.1 - https://cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf

[04] Top Threats to Cloud Computing V1.0 - https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf

[05] SaaS, PaaS, and IaaS: a Security Checklist for Cloud Models - http://www.csoonline.com/article/print/660065

[06] Cloud – 10 Risks with Cloud IT Foundation Tier - https://www.owasp.org/index.php/Cloud-10_Risks_with_Cloud_IT_Foundation_Tier

[07] Edward L. Haletky, "VMware vSphere and Virtual Infrastructure Security", Prentice Hall, 2009, ISBN-13: 978-0-137-15800-3.

[08] Cloud Computing and Security – A Natural Match - http://www.trustedcomputinggroup.org/files/resource_files/1F4DEE3D-1A4B-B294-D0AD0742BA449E07/Cloud%20Computing%20and%20Security%20Whitepaper_July29.2010.pdf.

[09] Symantec Internet Security Threat Report, Trends for 2010, Volume 16, April 2011.