Best Practices for Cloud Security and Privacy

Eric A. Hibbard, CISSP, CISA / Hitachi Data Systems

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA Education Committee.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

Abstract

Best Practices for Cloud Security and Privacy

As organizations embrace various cloud computing offerings it is important to address security and privacy as part of good governance, risk management and due diligence. Failure to adequately handle these requirements can place the organization at significant risk for not meeting compliance obligations and exposing sensitive data to possible data breaches. Fortunately, ISO/IEC, ITU-T and the Cloud Security Alliance (CSA) have been busy developing standards and guidance in these areas for cloud computing, and these materials can be used as a starting point for what some believe is a make-or-break aspect of cloud computing.

This session provides an introduction to cloud computing security concepts and issues as well as identifying key guidance and emerging standards. Specific CSA materials are identified and discussed to help address common issues. The session concludes by providing a security review of the emerging ISO/IEC and ITU-T standards in the cloud space.

Outline

- **Cloud Computing 101**
- Major Cloud Computing Threats
- Prevailing Cloud Security & Privacy Guidance
- Important Cloud Security & Privacy Resources
- Summary

Cloud Computing…

paradigm for enabling network access to a *scalable* and *elastic* pool of *shareable* physical or virtual resources with *self-service* provisioning and administration *on-demand*

SOURCE: ISO/IEC DIS 17788 | Draft Recommendation ITU-T Y.3500 Y.ccdef, *Cloud computing – Overview and vocabulary*, Oct-2013

Key Characteristics
(ISO/IEC DIS 17788)

- ***Broad network access*** – feature where the physical and virtual resources are available over a network and accessed through standard mechanisms that promote use by heterogeneous client platforms
- ***Measured Service*** – feature where the metered delivery of cloud services is such that usage can be monitored, controlled, reported, and billed
- ***Multi-tenancy*** – feature where physical or virtual resources are allocated in such a way that multiple tenants and their computations and data are isolated from and inaccessible to one another
- ***On-demand self-service*** – feature where a *cloud service customer* can provision computing capabilities, as needed, automatically or with minimal interaction with the *cloud service provider*
- ***Rapid elasticity & scalability*** – feature where physical or virtual resources can be rapidly and elastically provisioned, in some cases automatically, to quickly increase or decrease resources
- ***Resource pooling*** – feature where a cloud service provider's physical or virtual resources can be aggregated in order to serve one or more cloud service customers

Major Cloud Computing Roles
(ISO/IEC DIS 17788)

- **Cloud Service Customer**
  - *party which is in a business relationship for the purpose of using cloud services*
  - **Sub-roles:** Cloud Service User, Customer Cloud Service Administrator, Customer Business Manager, and Customer Cloud Service Integrator
- **Cloud Service Provider**
  - *party which makes cloud services available*
  - **Sub-roles:** Cloud Service Manager, Development Manager, Cloud Service Administrator, Customer Support & Care Representative, Business Manager, Security & Risk Administrator, Inter-cloud Provider
- **Cloud Service Partner**
  - *party which is engaged in support of, or auxiliary to, activities of either the cloud service provider or the cloud service customer, or both*
  - **Sub-roles:** Cloud Service Developer, Auditor, and Cloud Broker

Cloud Deployment Models
(ISO/IEC DIS 17788)

- **Private Cloud –** cloud deployment model that is used exclusively by a single cloud service customer where resources are controlled by that cloud service customer
- **Public Cloud –** cloud deployment model that is potentially available to any cloud service customer where resources are controlled by the cloud service provider
- **Hybrid Cloud –** deployment model of cloud computing using at least two different cloud deployment models
- **Community Cloud –** cloud deployment model that exclusively supports and is shared by a specific collection of cloud service customers who have shared requirements and a relationship with one another, and where resources are controlled by at least one member of this collection

Service Categories vs. Capability Types

(ISO/IEC DIS 17788)

Cloud Service Categories	Cloud Capabilities Types		
	Infrastructure	Platform	Application
Software as a Service			X
Platform as a Service		X	
Infrastructure as a Service	X		
Network as a Service	X	X	X
Data Storage as a Service	X	X	X
Compute as a Service	X		
Communication as a Service		X	X

■ ■ ■

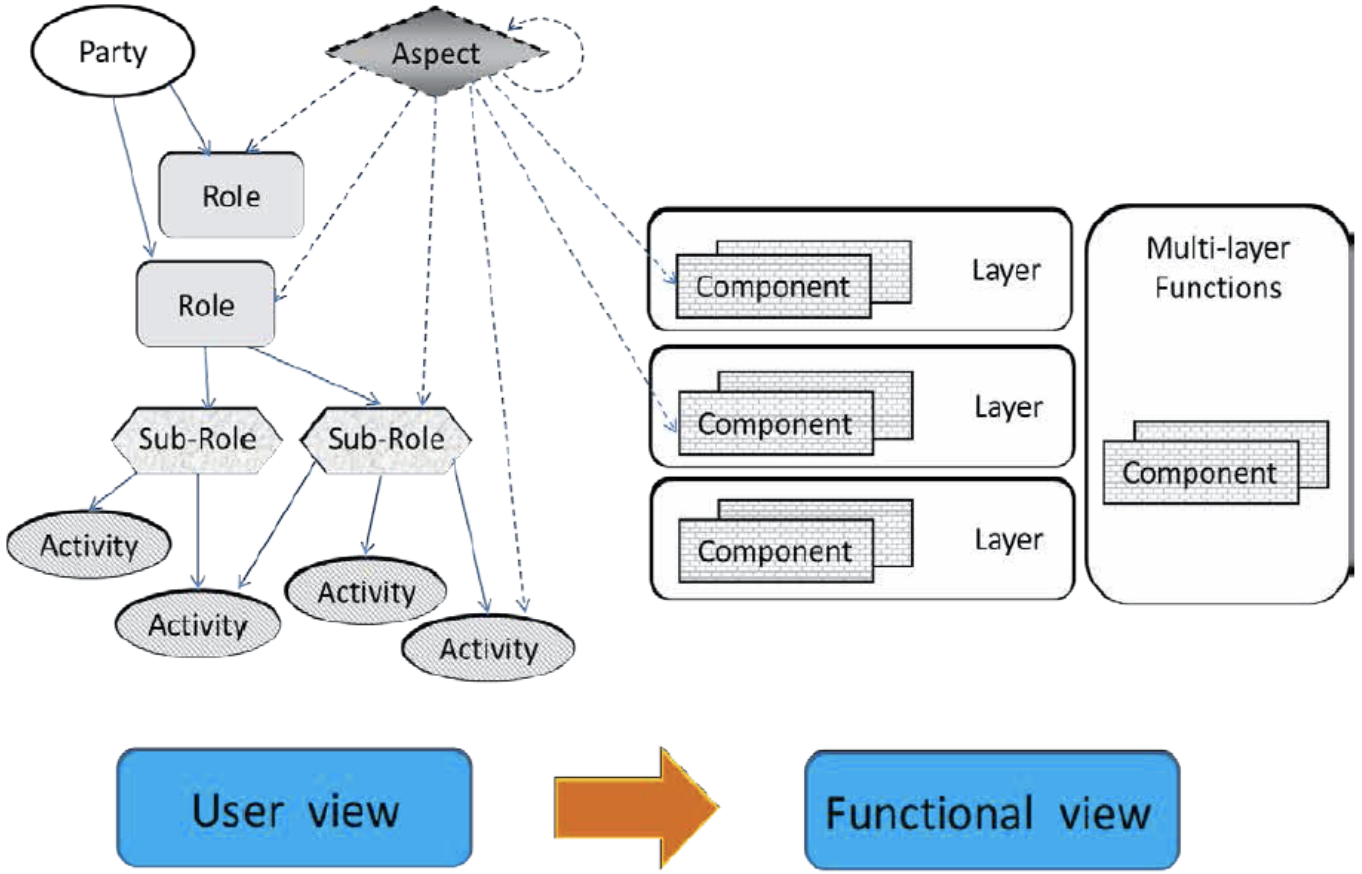
Washing-machine as a Service (WaaS)

Cross-cutting Aspects
(ISO/IEC DIS 17788)

- Auditability
- Availability
- Governance
- Interoperability
- Maintenance & Versioning
- Performance
- Portability
- Privacy
- Regulatory
- Resilience
- Reversibility
- Security
- Service levels and SLAs

Reference Architecture (1)

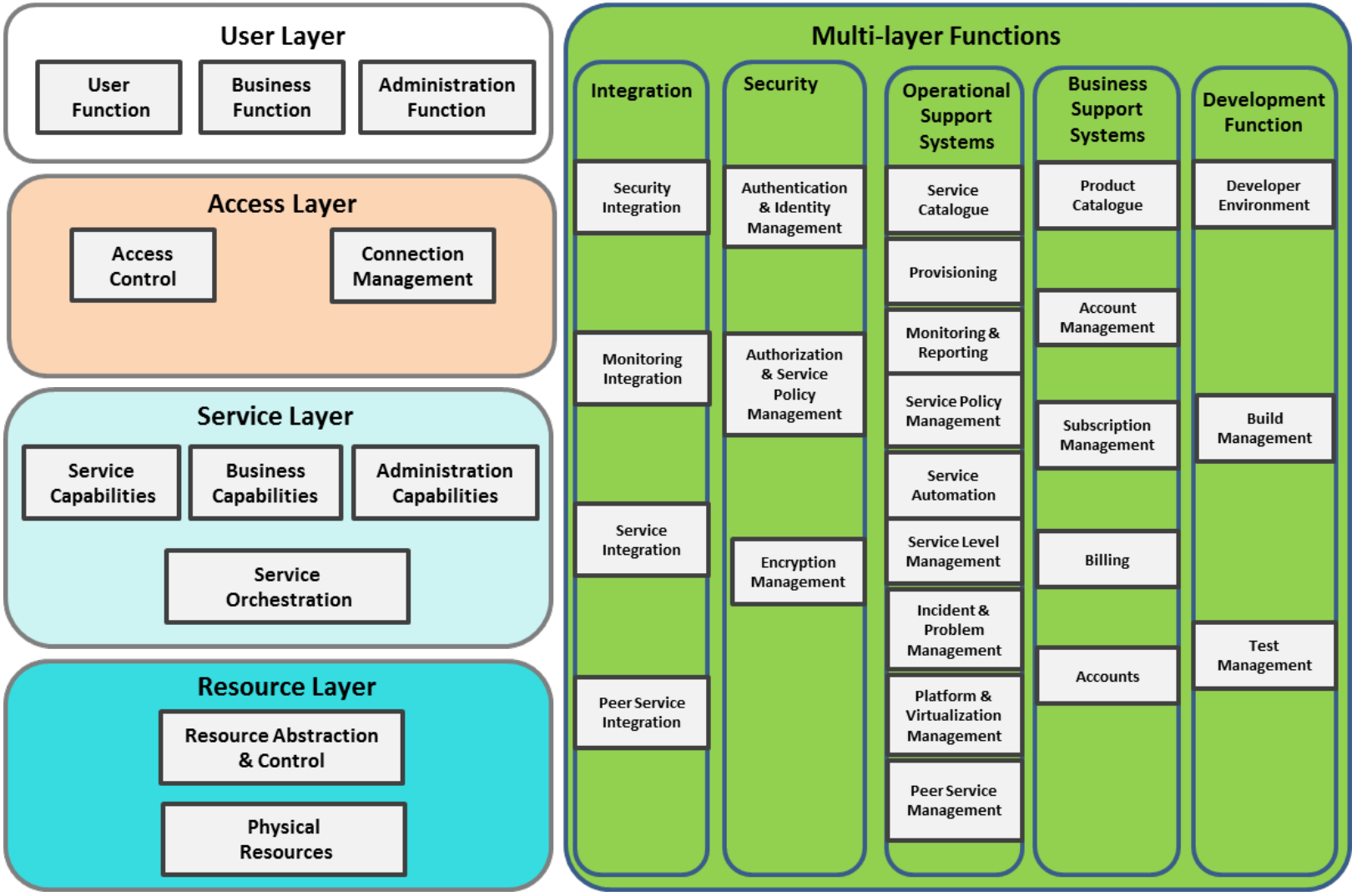
(ISO/IEC DIS 17789)



SOURCE: ISO/IEC DIS 17789 | Recommendation ITU-T Y.3502 Y.ccra, *Cloud computing – Reference architecture*, Oct-2013

Reference Architecture (2)

(ISO/IEC DIS 17789)



Outline

- Cloud Computing 101
- **Major Cloud Computing Threats**
- Prevailing Cloud Security & Privacy Guidance
- Important Cloud Security & Privacy Resources
- Summary

ITU-T X.1601 Threats

- For Cloud Service Customer
  - Data loss and leakage
  - Insecure service access
  - Insider threats
- For Cloud Service Providers
  - Unauthorized administration access
  - Insider threats

SOURCE: Recommendation ITU-T X.1601, *Security framework for cloud computing*, Jan-2014

ITU-T X.1601 Challenges

- For Cloud Service Customer
  - Ambiguity in Responsibility
  - Loss of Trust
  - Loss of Governance
  - Loss of Privacy
  - Service Unavailability
  - Cloud Service Provider Lock-in
  - Misappropriation of intellectual property
  - Loss of software integrity
- For Cloud Service Providers
  - Ambiguity in Responsibility
  - Shared Environment
  - Inconsistency and Conflict of Protection Mechanisms
  - Jurisdictional Conflict
  - Evolutionary Risks
  - Bad Migration and Integration
  - Business Discontinuity
  - Cloud Service Partner Lock-in
  - Supply Chain Vulnerability
  - Software Dependencies
  - Abuse Right of Cloud Service Provider
- For Cloud Service Partners
  - Ambiguity in Responsibility
  - Misappropriation of intellectual property
  - Loss of software integrity

CSA Top Threats

- #1: Data Breaches
- #2: Data Loss
- #3: Account Hijacking
- #4: Insecure APIs
- #5: Denial of Service
- #6: Malicious Insiders
- #7: Abuse of Cloud Services
- #7: Insufficient Due Diligence
- #9: Shared Technology Issues

SOURCE: Cloud Security Alliance (CSA), *The Notorious Nine: Cloud Computing Top Threats in 2013*, Feb-2013

Outline

- Cloud Computing 101
- Major Cloud Computing Threats
- **Prevailing Cloud Security & Privacy Guidance**
- Important Cloud Security & Privacy Resources
- Summary

Top Security Concerns with Cloud
(Customer Perspective)

- Data breaches involving sensitive data
- Understanding how cloud services provide for the following:
  - Preserving confidentiality, integrity and availability
  - Maintaining appropriate levels of identity and access control
  - Ensuring appropriate audit and compliance capability
- Dealing with loss of control; physical and logical access
- Trusting the cloud service provider
- Incident management and response
- Data reversibility

Cloud Standards Customer Council

Security for Cloud Computing – 10 Steps to Ensure Success

SNIA Education

01: Ensure effective governance, risk and compliance processes exist
02: Audit operational & business processes
03: Manage people, roles and identities
04: Ensure proper protection of data and information
05: Enforce privacy policies
06: Assess the security provisions for cloud applications
07: Ensure cloud networks and connections are secure
08: Evaluate security controls on physical infrastructure and facilities
09: Manage security terms in the cloud SLA
10: Understand the security requirements of the exit process

SOURCE: Cloud Standards Customer Council, *Security for Cloud Computing – 10 Steps to Ensure Success*, August 2012, http://www.cloud-council.org

Cloud Security (or Insecurity)

- Core Information Assurance issues to address:
  - Confidentiality
  - Integrity
  - Availability
  - Possession
  - Authenticity
  - Utility
  - Privacy
  - Authorized use
  - Non-repudiation
- Data loss and/or leakage measures become even more important
- Data aggregation changes the risk equation
- Legal and compliance forces require additional due diligence
- Forced exits and data disposition have to be carefully thought out
- Incident management become much more complicated

Privacy

- Many countries—the U.S. being a notable exception—consider privacy to be a fundamental human right
- Privacy protection laws have been introduced in a significant number of countries
- The types of "protected" data can vary significantly
- Privacy violations can include the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorized disclosure of such data
- There may be cross-border restrictions imposed on data
- European Commission's proposal for cloud:
  - New rights (to be forgotten/data deletion and data portability)
  - *Privacy by Default* and *Privacy by Design*
  - *Security obligations and data breach notification regime*

ISO/IEC 29100 Privacy Principles

- 1. Consent and choice
- 2. Purpose legitimacy and specification
- 3. Collection limitation
- 4. Data minimization
- 5. Use, retention and disclosure limitation
- 6. Accuracy and quality
- 7. Openness, transparency and notice
- 8. Individual participation and access
- 9. Accountability
- 10. Information security
- 11. Privacy compliance

Jurisdictional Fog

- It has been said that possession is nine tenths of the law…that may not be the case for cloud
- It is often the situation that an entity has to have some physical presence in a country in order for a government to obtain access to the entity's data
- In the era of the cloud, however, all that may be required is a physical presence of the "cloud provider"
- This is not limited to just the U.S. Patriot Act (other law enforcement authorities have invoked similar provisions)

Litigating in the Cloud

Digital Evidence and Forensics

- Amassing the forensic data from the various sources could be a serious challenge
- Real-time nature of cloud services may reduce the amount and nature of digital evidence
- The integrity and authenticity of data may be questionable (for example, inadequate protections against attacks)

Electronic Discovery

- Organizations will have additional challenges identifying relevant data because business units are directly leveraging the Cloud
- Relevant data could be within the hands of a large number of third parties (suppliers to suppliers)

Possible Security Benefits
(Especially for SMBs)

- Centralized data
- Segmented data and applications
- Better logging/accountability
- Standardized images for asset deployment
- Better resilience to attack & streamlined incident response
- More streamlined audit and compliance
- Better visibility to process
- Faster deployment of applications, services, etc.

Outline

- Cloud Computing 101
- Major Cloud Computing Threats
- Prevailing Cloud Security & Privacy Guidance
- **Important Cloud Security & Privacy Resources**
- Summary

ISO/IEC JTC 1

(Information technology Standards)

- **Subcommittee 38:**
  - ISO/IEC 17826:2012, *Information technology - Cloud Data Management Interface (CDMI)*
- **Subcommittee 27:**
  - ISO/IEC CD 27017, *Information technology – Security techniques – Code of practice for information security controls for cloud computing services based on ISO/IEC 27002*
  - ISO/IEC DIS 27018, *Information technology – Security techniques – – Code of practice for PII protection in public clouds acting as PII processors*
  - ISO/IEC 3rdWD 27036-4, *Information technology – Security techniques – Information security for supplier relationships – Part 4: Guidelines for security of cloud services*
  - ISO/IEC DIS 27040, *Information technology – Security techniques – Storage Security*

Subcommittee 27
(Security techniques)

- **ISO/IEC 27017**
  - Additional implementation guidance for relevant information security controls specified in ISO/IEC 27002
  - Additional controls and implementation guidance that specifically relate to cloud computing services.
- **ISO/IEC 27018**
  - Applies to organizations providing public cloud computing services that act as PII processors (possibly PII controllers)
  - Establishes commonly accepted control objectives, controls and guidelines for implementing controls to protect
- **ISO/IEC 27036-4**
  - Define guidelines supporting the implementation of Information Security Management for the use of cloud service
- **ISO/IEC 27040**
  - Addresses general storage security issues, including cloud storage and CDMI guidance

ITU-T/Study Group 17 (SG17)

- ***X.1601 (X.ccsec)*** – High-level security framework for cloud computing
- ***X.cc-control (ISO/IEC 27017)*** – Guidelines supporting the implementation of information security controls for cloud service providers and cloud service customers of cloud computing services
- ***X.goscc*** – Guidelines of operational security for cloud computing
- ***X.sfcse*** – Security functional requirements for Software as a Service (SaaS) application environment
- ***X.ccidm*** – Requirement of IdM in cloud computing

Cloud Security Alliance (CSA)

- Security Guidance for Critical Areas of Focus in Cloud Computing
- Open Certification Framework
- Cloud Controls Matrix (CCM)
- Trusted Cloud Initiative (TCI) Reference Architecture Model
- Top Threats to Cloud Computing
- Security as a Service (SecaaS) Implementation Guidance
- Privacy Level Agreement (PLA)

- Many others…

CSA Cloud Security Guidance

Governance	Operations
Governance and Enterprise Risk Management	Traditional Security, Business Continuity and Disaster Recovery
Legal and Electronic Discovery	Data Center Operations
Compliance and Audit	Incident Response, Notification and Remediation
Information Lifecycle Management	Application Security
Portability and Interoperability	Encryption and Key Management
	Identity and Access Management
	Virtualization

NOTE: The governance domains are broad and address strategic and policy issues within a cloud computing environment, while the operational domains focus on more tactical security concerns and implementation within the architecture.

SOURCE: Cloud Security Alliance, *Security Guidance for Critical Areas of Focus in Cloud Computing*, Version 3.0, 2011, http://www.cloudsecurityalliance.org

CSA GRC Stack

- Cloud Controls Matrix (CCM)
  - Provides mappings on
    - Architectural relevance (Physical, Network, Compute, Storage, Application, Data and Corporate Governance)
    - Delivery Models (SaaS, PaaS, IaaS)
    - Supplier relationships (Service Provider and Tenant)
    - Scope Applicability
  - Work underway to align with ISO/IEC 27001:2013
- CloudAudit
- Consensus Assessments Initiative Questionnaire (CAIQ)
- Cloud Trust Protocol (CTP)

SOURCE: Cloud Security Alliance, GRC Stack, https://cloudsecurityalliance.org/research/grc-stack/

CSA CCM v3 Control Domains

- Application & Interface Security [4]
- Audit Assurance & Compliance [3]
- Business Continuity Management & Operational Resilience [12]
- Change Control & Configuration [5]
- Data Security & Information Lifecycle Management [8]
- Datacenter Security [9]
- Encryption & Key Management [4]
- Governance and Risk Management [12]
- Human Resources [12]
- Identity & Access Management [13]
- Infrastructure & Virtualization Security [12]
- Interoperability & Portability [5]
- Mobile Security [20]
- Security Incident Management, E-Discovery & Cloud Forensics [5]
- Supply Chain Management, Transparency and Accountability [9]
- Threat and Vulnerability Management [3]

CSA Privacy Level Agreement (1)

(Sale of Cloud Services in the EU)

1) Identity of the CSP
2) Categories of personal data that the customer is prohibited from sending to or processing in the cloud
3) Ways in which the data will be processed
4) Data transfer
5) Data security measures
6) Monitoring
7) Third-party audits
8) Personal data breach notification

SOURCE: Cloud Security Alliance, *Privacy Level Agreement Outline for the Sale of Cloud Services in the European Union*, February 2013, https://cloudsecurityalliance.org/research/grc-stack/

CSA Privacy Level Agreement (2)

(Sale of Cloud Services in the EU)

9) Data portability, migration, and transfer-back assistance
10) Data retention, restitution, and deletion
11) Accountability
12) Cooperation
13) Law enforcement access
14) Remedies
15) Complaint and dispute resolution
16) CSP insurance policy

NIST – Cloud Computing

- ***Special Publication 800-144***, Guidelines on Security and Privacy in Public Cloud Computing
- ***Special Publication 800-145***, The NIST Definition of Cloud Computing
- ***Special Publication 800-146***, Cloud Computing Synopsis and Recommendations
- ***Special Publication 500-291***, NIST Cloud Computing Standards Roadmap
- ***Special Publication 500-292***, NIST Cloud Computing Reference Architecture
- ***Special Publication 500-293***, (Draft). US Government Cloud Computing Technology Roadmap, Volume I High-Priority Requirements to Further USG Agency Cloud Computing Adoption
- ***Special Publication 500-293***, (Draft). US Government Cloud Computing Technology Roadmap, Volume II Useful Information for Cloud Adopters
- ***Special Publication 500-299***, (Draft) NIST Cloud Computing Security Reference Architecture
- ***Interagency Report 7904***, (Draft) Trusted Geolocation in the Cloud: Proof of Concept Implementation

FedRAMP

- Federal Risk and Authorization Management Program (FedRAMP)
- US Government-wide program
  - provides a standardized approach to security assessment,
  - authorization, and
  - continuous monitoring for cloud products and services.
- Relevant for
  - Cloud Service Providers (CSPs),
  - Third Party Assessment Organizations (3PAOs),
  - government employees and contractors working on FedRAMP projects, and
  - any outside organizations that want to use or understand the FedRAMP assessment process.
- More information at:
  http://www.gsa.gov/portal/category/102371

FedRAMP Security Controls

- Access Control (AC)
- Awareness & Training (AT)
- Audit & Accountability (AU)
- Assessment & Authorization (CA)
- Configuration Management (CM)
- Contingency Planning (CP)
- Identification & Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Physical & Environmental Protection (PE)
- Planning (PL)
- Risk Assessment (RA)
- System & Services Acquisition (SA)
- System & Communications Protection (SC)
- System & Information Integrity (SI)

NOTE: Security controls were selected from the NIST catalog of controls and enhancements as described in Special Publication 800-53 as revised

Other Resources

- SNIA Cloud Storage Initiative, http://www.snia.org/cloud
- European Network and information Security Agency (ENISA), *Cloud Computing – Benefits, risks and recommendations for information security*, http://www.enisa.europa.eu/
- Information Systems Audit and Control Association (ISACA), *Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives*, http://www.isaca.org

Outline

- Cloud Computing 101
- Major Cloud Computing Threats
- Prevailing Cloud Security & Privacy Guidance
- Important Cloud Security & Privacy Resources
- **Summary**

Cloud Security Tips

- Cloud-based security is not a substitute for existing ICT security…think defense in depth
- Understand the Terms of Service…this is the best you can expect
- Don’t put anything in the cloud you wouldn’t want someone else to see (government, competitor, or a private litigant)
- Placing consumer data in the cloud could put you at risk of violating the law…where is it?

Final Thoughts

- It is *possible* to engineer solutions across most cloud services today that meet or exceed the security provided within the enterprise…however, the capability to execute may not be a reality!
- The various value propositions of cloud (agility, low cost, scalability, security) are often conflated, suggesting all four can be achieved simultaneously and in equal proportions; this is a fallacy because trade-off are almost always required.

SNIA Security Organizations

- SNIA Security Technical Work Group (TWG)
  - Focus: Requirements, architectures, interfaces, practices, technology, educational materials, and terminology for storage networking.
  - http://www.snia.org/tech_activities/workgroups/security/
- Storage Security Industry Forum (SSIF)
  - Focus: Educational materials, customer needs, whitepapers, and best practices for storage security.
  - http://www.snia.org/ssif

Attribution & Feedback

The SNIA Education Committee thanks the following individuals for their contributions to this Tutorial.

Authorship History

Authors (Spring 2014)

Eric Hibbard, CISSP, CISA

(incorporating materials from earlier tutorial dating back to 2012)

Additional Contributors

SNIA Security TWG

CSA International Standardization Council

ABA SciTech Cloud Computing Committee

Please send any questions or comments regarding this SNIA Tutorial to ***tracktutorials@snia.org***