Architecting Data Services for the Cloud

Security Considerations and Best Practices

Dr Adnene Guabtni, Senior Research Scientist, Data61, CSIRO

Adnene.Guabtni@csiro.au

Did you say Cloud?

29% of the general public think Cloud Technology is an actual cloud (Wakefield Research)

So, let's talk about what IT professionals think about the cloud.

- For IT professionals the benefits of the cloud are:
  - Portable office.
  - Cost Savings.
  - Fewer responsibilities,
  - easier manageability.
  - Reliability (SLA which guarantees 24/7/365 and 99.99% availability).
- Looks like traditional “Hosted services”.

The Cloud Computing Difference

IT Assets Become Programmable Resources

- Servers, databases, storage, and higher-level application components are temporary and disposable, quickly provisioned when needed.
- They dynamically scale to meet actual demand.
- You only pay for what you use.

Think of how a software allocates memory on demand and “garbage collect” unused objects?
Cloud Computing is similar but applied to virtual resources like servers, databases, storage, …

The Cloud Computing Difference

IT Assets Become Programmable Resources

No need to know how to program resources

- Rely on a higher level of managed services, such as Auto-scaling, Load balancers, ...
- Deliver new solutions faster.
- Designed for scalability and high availability.

The Cloud Computing Difference

IT Assets Become Programmable Resources

No need to know how to program resources

Global, Available, and Unlimited Capacity

- Whether you need to serve 1 user or 1 billion users.
- Whether you need to optimize network speed for US, Europe, Asia, etc.
- Move machines and data around the globe programmatically.
- Business Continuity.
- Disaster recovery.

The Cloud Computing Difference

IT Assets Become Programmable Resources

No need to know how to program resources

Global, Available, and Unlimited Capacity

Security is Built-in

- Native AWS security and encryption features can help achieve higher levels of data protection and compliance.
- Security policies built-into programmable resources.
- Continuous monitoring of configuration changes to your IT resources.
- Auditing is no longer periodic or manual, it becomes part of your continuous delivery pipeline.

The Cloud Computing Difference

IT Assets Become Programmable Resources

No need to know how to program resources

Global, Available, and Unlimited Capacity

Security is Built-in

Recommended reading

AWS Security Best Practices

White paper from Amazon Web Services, August 2016.

https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Best_Practices.pdf

Other cloud providers have also excellent security guidelines and best practices. For example:

- Azure security best practices and patterns
  https://docs.microsoft.com/en-us/azure/security/security-best-practices-and-patterns
- Google Cloud - Best Practices for Enterprise Organizations
  https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations

Cloud security: conceptions and misconceptions

- **The cloud takes care of all my security considerations**

  NO The Cloud provides the building blocks that customers can use to achieve their security goals. Providers of bricks are not responsible for the safety of poorly built houses. You are the architect and you are responsible for what you build.

- **The cloud is secure by default.**

  NO Default settings are often not secure. The cloud provider is choosing between convenience and ease of use on the one hand, and security on the other hand. The default settings are often leaning towards convenience.

- **The cloud is insecure because it uses shared physical infrastructure.**

  NO Virtualization technologies are very reliable at isolating virtual resources from one another. Furthermore, the integrity and security of the physical infrastructure in cloud data centers are among the best in the world. More is being done by hardware manufacturers to improve this further (e.g. AMD EPYC server chip).

Cloud security is a shared responsibility

AWS shared responsibility model

The Cloud provider manages the security of the following assets:

- Facilities
- Physical security of hardware
- Network infrastructure
- Virtualization infrastructure

The Customer is responsible for the security of the following assets:

- Amazon Machine Images (AMIs)
- Operating systems
- Applications
- Data in transit and at rest
- Data stores
- Credentials
- Policies and configuration

Cloud security is a shared responsibility

Example 1. You are running a virtual machine on EC2 (Elastic Compute Cloud)

The cloud provider controls the physical security of hardware

You control the operating system running on the VM and you have to configure it adequately to secure your data. You also control who can access the services deployed on your VM (RSA keys).

Example 2. You are using a Container Service (or managed service)

Examples of container services include Amazon Relational Database Services (Amazon RDS), Amazon Elastic Map Reduce (Amazon EMR) and AWS Elastic Beanstalk to run apps.

While you are not controlling the operating system running the container service, you have quite a lot of controls such as setting up and managing network controls (firewall rules), and for managing platform-level identity and access management.

Cloud security is a shared responsibility

Example 3. You are using Abstracted Services

Examples of abstracted services include Amazon Simple Storage Service (Amazon S3), Amazon Glacier, Amazon DynamoDB, Amazon Simple Queuing Service (Amazon SQS), and Amazon Simple Email Service (Amazon SES).

These services abstract the platform or management layer on which you can build and operate cloud applications. You access the endpoints of these abstracted services using AWS APIs, and AWS manages the underlying service components or the operating system on which they reside.

This is the lowest level of responsibility for the customer. However you are still responsible for managing your data access (e.g. what data to expose, who can access it). Also, there are very little scenarios in which customers will only use abstracted services, so combining them with container services and VM is often the case.

Design an Information Security Management System for your Cloud assets

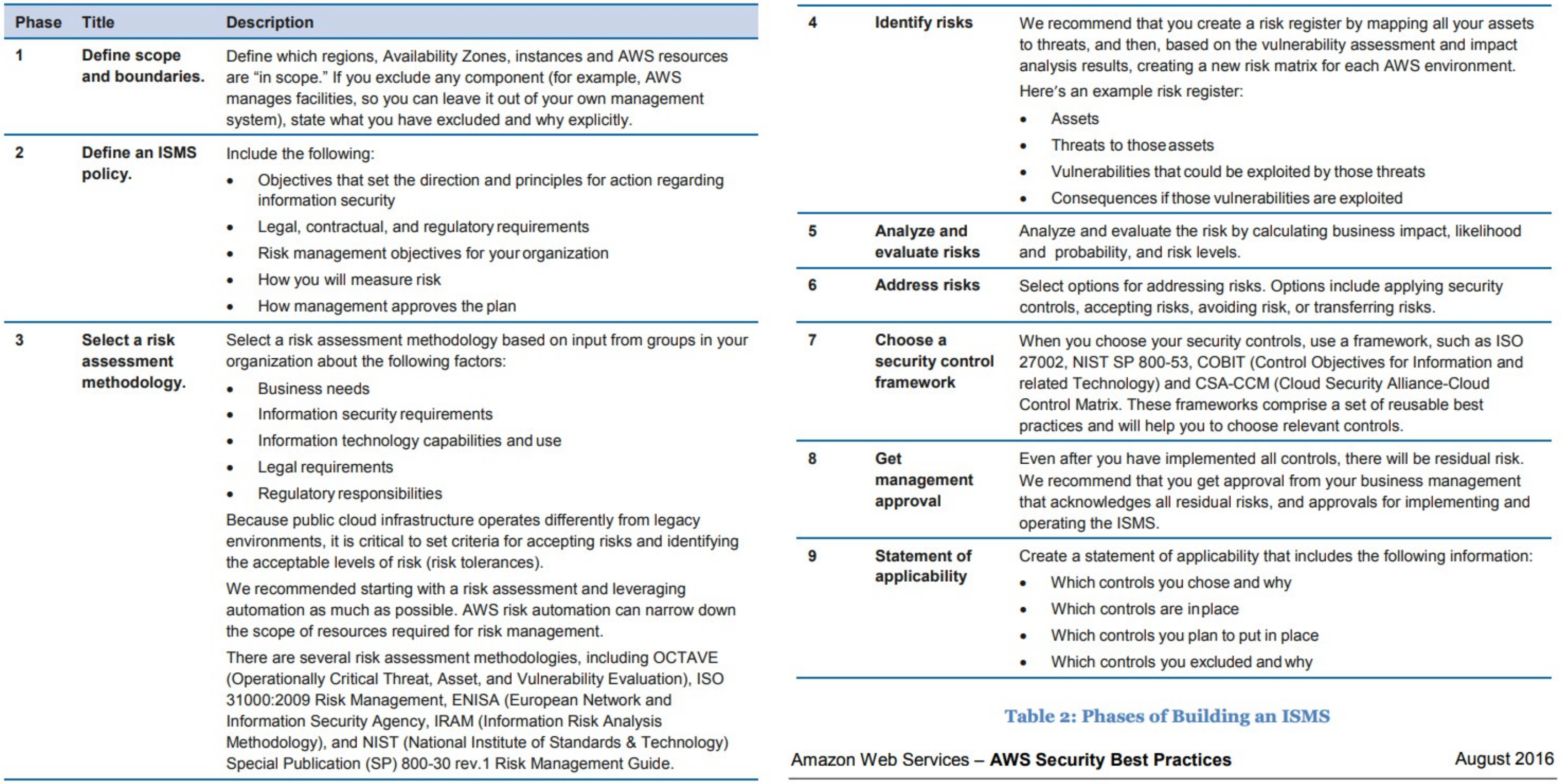
An ISMS is the collection of information security policies and processes for your organization’s assets (on the cloud).

Security requirements differ in every organization, depending on the following factors:

- Business needs and objectives
- Processes employed
- Size and structure of the organization

Standard frameworks, such as ISO 27001, are helpful with ISMS design and implementation.

Design an Information Security Management System for your Cloud assets



Phase	Title	Description
1	**Define scope and boundaries.**	Define which regions, Availability Zones, instances and AWS resources are “in scope.” If you exclude any component (for example, AWS manages facilities, so you can leave it out of your own management system), state what you have excluded and why explicitly.
2	**Define an ISMS policy.**	Include the following: • Objectives that set the direction and principles for action regarding information security • Legal, contractual, and regulatory requirements • Risk management objectives for your organization • How you will measure risk • How management approves the plan
3	**Select a risk assessment methodology.**	Select a risk assessment methodology based on input from groups in your organization about the following factors: • Business needs • Information security requirements • Information technology capabilities and use • Legal requirements • Regulatory responsibilities Because public cloud infrastructure operates differently from legacy environments, it is critical to set criteria for accepting risks and identifying the acceptable levels of risk (risk tolerances). We recommended starting with a risk assessment and leveraging automation as much as possible. AWS risk automation can narrow down the scope of resources required for risk management. There are several risk assessment methodologies, including OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), ISO 31000:2009 Risk Management, ENISA (European Network and Information Security Agency, IRAM (Information Risk Analysis Methodology), and NIST (National Institute of Standards & Technology) Special Publication (SP) 800-30 rev.1 Risk Management Guide.
4	**Identify risks**	We recommend that you create a risk register by mapping all your assets to threats, and then, based on the vulnerability assessment and impact analysis results, creating a new risk matrix for each AWS environment. Here’s an example risk register: • Assets • Threats to those assets • Vulnerabilities that could be exploited by those threats • Consequences if those vulnerabilities are exploited
5	**Analyze and evaluate risks**	Analyze and evaluate the risk by calculating business impact, likelihood and probability, and risk levels.
6	**Address risks**	Select options for addressing risks. Options include applying security controls, accepting risks, avoiding risk, or transferring risks.
7	**Choose a security control framework**	When you choose your security controls, use a framework, such as ISO 27002, NIST SP 800-53, COBIT (Control Objectives for Information and related Technology) and CSA-CCM (Cloud Security Alliance-Cloud Control Matrix. These frameworks comprise a set of reusable best practices and will help you to choose relevant controls.
8	**Get management approval**	Even after you have implemented all controls, there will be residual risk. We recommend that you get approval from your business management that acknowledges all residual risks, and approvals for implementing and operating the ISMS.
9	**Statement of applicability**	Create a statement of applicability that includes the following information: • Which controls you chose and why • Which controls are in place • Which controls you plan to put in place • Which controls you excluded and why

Table 2: Phases of Building an ISMS

Amazon Web Services – **AWS Security Best Practices** August 2016

Divide and rule your cloud assets

Design your cloud account management strategy with security in mind by creating multiple cloud accounts for:

- Separate environments (production, development, and testing)
- Multiple autonomous departments
- Multiple autonomous independent projects

AWS offers consolidated billing so that you don't have to setup billing for each account separately.

Strengthen your authentication

- Use Multi-factor authentication (MFA)
- Rotate their access keys on a regular basis
- Use Temporary Security Credentials for applications requiring access to cloud assets. These temporary security credentials have a configurable expiration and are automatically rotated.

Secure your data at rest

- Encrypt your data in the cloud
  - For regulatory or business requirements, you might want to encrypt your data at rest stored in the cloud to protect against accidental or unlawful information disclosure. Use both server side and client side encryption.
  - Select the right encryption method
  - Store and Manage Encryption Keys safely in tamper-proof storage, such as Hardware Security Modules (e.g AWS CloudHSM). You can also store keys on premises and access them over secure links.
  - If you are using a VM, you can also implement Encrypted File System (EFS) on Windows or dm-crypt on Linux.

Secure your data at rest

- Use resource permissions and versioning to limit risks of data integrity compromise or accidental deletion.
- Use data backup and replication to protect against system, infrastructure, hardware or software unavailability

Secure your data in transit

- Encrypt data in transit using IPSec ESP and/or SSL/TLS to avoid accidental information disclosure and data integrity compromise.
  - Use HTTPS (HTTP over SSL/TLS) with server certificate authentication.
  - Offload HTTPS processing on Elastic Load Balancing to minimize impact on web servers while still protecting data in transit.
- Protect your data in transit against Peer identity compromise/identity spoofing/man-in-the-Middle attacks.
  - Use IPSec with IKE with pre-shared keys or X.509 certificates to authenticate the remote end. Alternatively, use SSL/TLS with server certificate authentication based on the server common name (CN), or Alternative Name (AN/SAN).

Secure your operating systems and applications

For VM (EC2 instances)

- Disable root API access keys and secret key
- Restrict access to instances from limited IP ranges using Security Groups
- Password protect the .pem file on user machines
- Delete keys from the authorized_keys file on your instances when someone leaves your organization or no longer requires access
- Rotate credentials (DB, Access Keys)
- Regularly run least privilege checks using IAM user Access Advisor and IAM user Last Used Access Keys

Secure your operating systems and applications

For Web Applications

- Use WAF (Web Application Firewall) to protect against SQL injection and other vulnerabilities.
- Setting up SSL on an Elastic Load Balancer which allows to offload your instances from managing SSL encryption/decryption.
  - Your SSL certificates are safe, within ELB, not within your instances.
  - Cypher suite configuration is always up to date, upgraded by Amazon when necessary (in case of new vulnerability).

Secure your cloud infrastructure

- Use VPC (Virtual Private Cloud)
  - This is a logically isolated section of Amazon Web Services (AWS) Cloud.
- Use bastion hosts to enforce control and visibility
  - A bastion host is a purpose server instance that is designed to be the primary access point and acts as a proxy to your other server instances in the cloud).
- Use Security Zoning and Network Segmentation
  - It is a security best practice to segment infrastructure into zones that impose similar security controls.
  - This can be achieving using multiple VPCs with separate security groups.

Building Threat Protection Layers

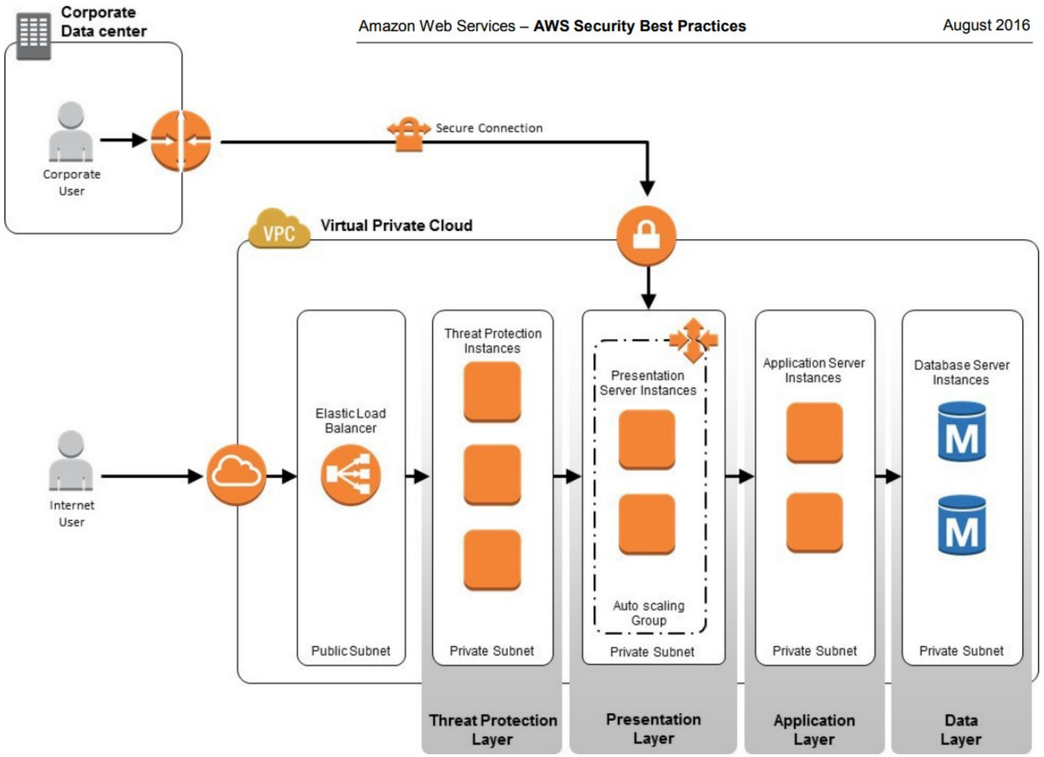


Figure 6: Layered Network Defense in the Cloud

Examples of inline threat protection technologies include the following:

- Third-party firewall devices installed on Amazon EC2 instances
- Unified threat management (UTM) gateways
- Intrusion prevention systems
- Data loss management gateways
- Anomaly detection gateways
- Advanced persistent threat detection gateways

Testing your Information Security Management System

- Every ISMS must ensure regular reviews of the effectiveness of security controls and policies.
- You should undertake a number of test approaches:
  - External Vulnerability Assessment (by a third party with little or no knowledge of the infrastructure and its components)
  - External Penetration Tests (by a third party with little or no knowledge of the infrastructure and its components)
  - Internal Gray/White-box Review of Applications and Platforms (by internal tester with some of full knowledge of the infrastructure and its components)

Thank you for your attention

Access these slides on SlideShare

slideshare.net/guabtni

Dr Adnene Guabtni, Senior Research Scientist, Data61, CSIRO

Adnene.Guabtni@csiro.au