Managing Cloud Computing Security & Risk

Module 3

117

Module Content

Content in this module comes from the following domains in CSA's Security Guidance and covers the following subject areas:

- **Domain 2 //** Governance and Enterprise Risk Management
- **Domain 3 //** Legal Issues, Contracts and Electronic Discovery
- **Domain 4 //** Compliance and Audit Management
- **Domain 5 //** Information Governance

- Risk and governance
- Legal and compliance
- Audit
- Data governance

CSA cloud security alliance®

118

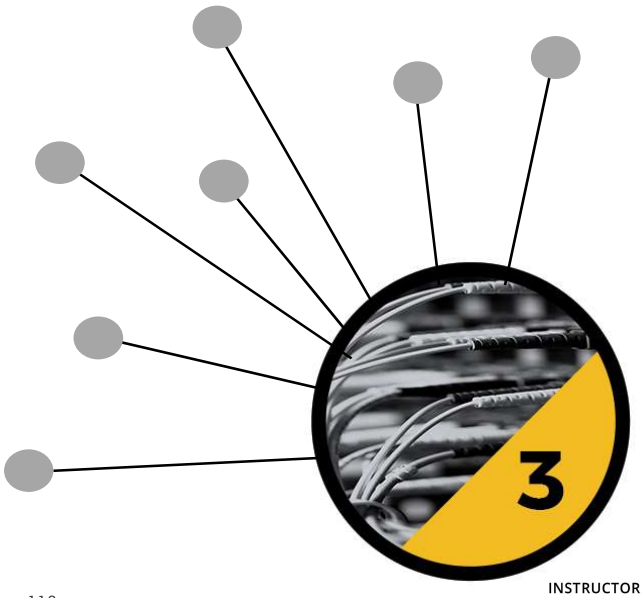
INSTRUCTOR LOGO HERE
Change img on all slide masters.

118

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Module Structure

Unit 1 // Module Into
Unit 2 // Governance
Unit 3 // Risk
Unit 4 // Compliance
Unit 5 // Legal Considerations for Cloud
Unit 6 // Audit
Unit 7 // CSA Tools



cloud security alliance

119

INSTRUCTOR LOGO HERE
Change img on all slide masters.

119

Objectives

The implications of cloud on governance, with a focus on contracts and controls.

How cloud affects enterprise risk management.

Some top-level legal areas cloud tends to affect (but not legal advice).

Managing compliance and audits for cloud deployments.

Tools from the Cloud Security Alliance to help assess and manage risk.

cloud security alliance

120

INSTRUCTOR LOGO HERE
Change img on all slide masters.

120

Copyright 2019 Cloud Security Alliance and Securosis, LLC

BEFORE WE BEGIN…

This module and the Guidance focus on how cloud computing affects governance, risk, and compliance (GRC). They are not designed to educate you on GRC fundamentals.

CSA cloud security alliance®

121

INSTRUCTOR LOGO HERE
Change img on all slide masters.

121

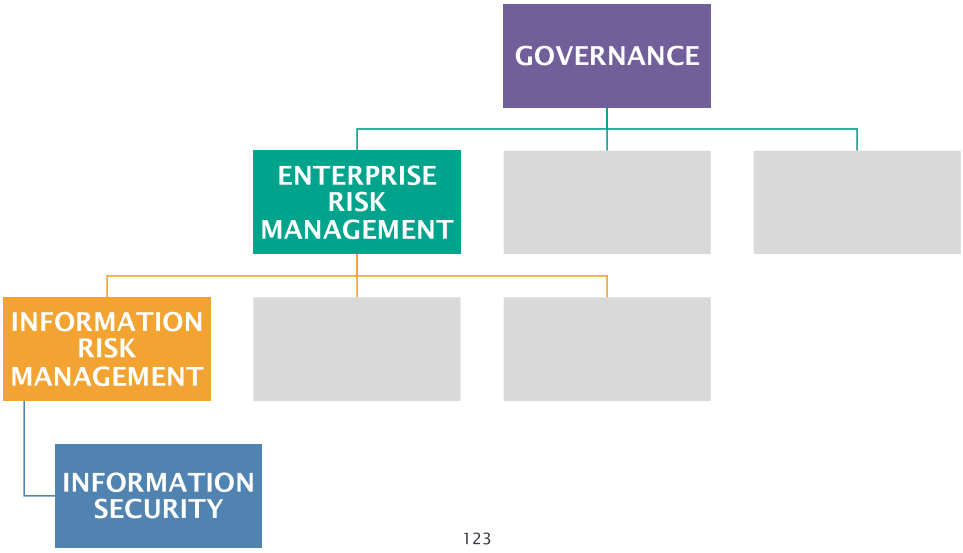
Governance

MODULE 3 // UNIT 2

122

Copyright 2019 Cloud Security Alliance and Securosis, LLC

A Simplified Hierarchy



cloud security alliance®

123

INSTRUCTOR LOGO HERE
Change img on all slide masters.

123

Tools of Cloud Governance

cloud security alliance®

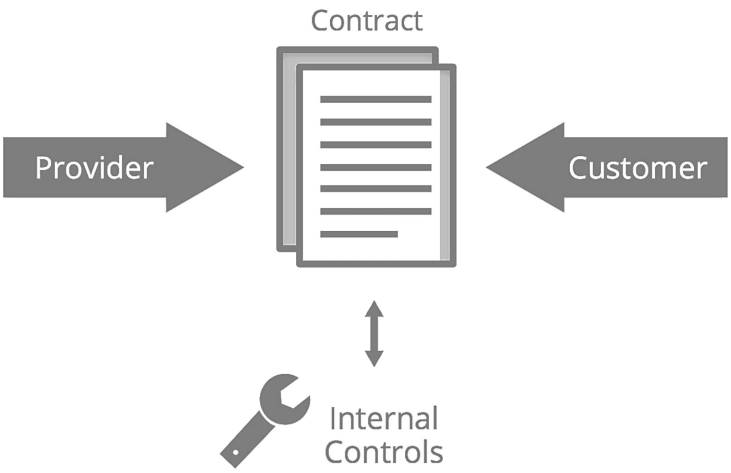
124

INSTRUCTOR LOGO HERE
Change img on all slide masters.

124

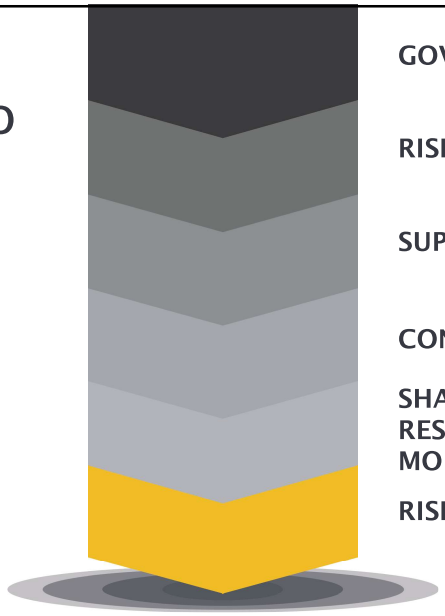
Copyright 2019 Cloud Security Alliance and Securosis, LLC

The Contract



125

From Governance To Risk



GOVERNANCE

RISK TOLERANCE

SUPPLIER ASSESSMENT

CONTRACTS

SHARED RESPONSIBILITIES MODEL

RISK MANAGEMENT

126

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Review

1. Governance defines how an organization is managed.
2. Contracts can extend governance and internal controls to the cloud provider.
3. The contract helps define the roles of the shared responsibilities model.
4. Supplier assessments and compliance reports help validate that the cloud provider is meeting the expectations of the cloud consumer.

cloud security alliance

127

INSTRUCTOR LOGO HERE
Change img on all slide masters.

127

128

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Risk Management

Enterprise Risk Management

- Rooted in providing value to stakeholders.
- How to measure, manage, and mitigate uncertainty.

Information Risk Management

- Aligning risk management to the tolerance of the data owner.
- Primary means of decision support for IT/security on the CIA of information assets.

CSA cloud security alliance®

129

INSTRUCTOR LOGO HERE
Change img on all slide masters.

129

Risk Assessment

CSA cloud security alliance®

130

INSTRUCTOR LOGO HERE
Change img on all slide masters.

130

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Service Model Effects

INFRASTRUCTURE AS A SERVICE (IAAS)

- Closest to traditional data center
- Most existing risk controls/activities will transfer
- Key differences are metastructure and abstraction/orchestration

PLATFORM AS A SERVICE (PAAS)

- Less likely to have fully negotiated contract
- May be difficult to measure contract compliance (SLAs)
- Much comes down to the details of the PaaS and how you integrate

SOFTWARE AS A SERVICE (SAAS)

- Nearly fully reliant on the contract to define governance/risk since you rely on the provider for nearly everything
- Big variation in maturity in the market
- Often limited to what you see in the UI

CSA cloud security alliance®

131

INSTRUCTOR LOGO HERE
Change img on all slide masters.

131

Deployment Model Effects

Public Cloud Environment

- Reduced ability to govern ops
- Reduced ability to negotiate contracts
- Shared responsibilities model

Community/Hybrid Environment

- Now have to calculate across 2 sets of contracts
- Or are dealing with group-negotiated contract and potential of differing priorities

Private Cloud Environment

- Governance/risk issues may be similar to public if third-party managed/hosted
- Provider may not negotiate contracts once terms set; e.g,. won't patch in timely manner
- Internal SLAs still used in private

CSA cloud security alliance®

132

INSTRUCTOR LOGO HERE
Change img on all slide masters.

132

Copyright 2019 Cloud Security Alliance and Securosis, LLC

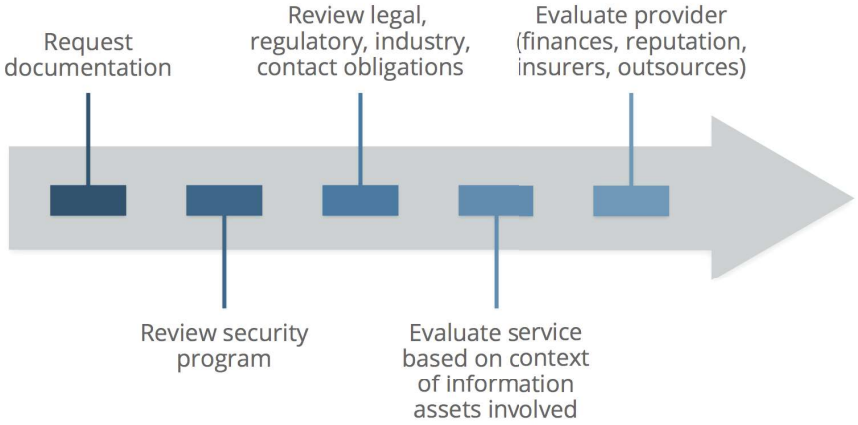
Tradeoff Considerations

Less
- Physical control over assets.
- Need to manage risks the provider accepts.

More
- Reliance on SLA and contract.
- Requirement to manage the relationship and stay up to date.
- Assessment instead of testing.

133

Cloud Risk Management Tools



134

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Governance & Risk Recommendations

Identify the shared responsibilities of security and risk management based on the chosen cloud deployment and service model.

Develop a cloud governance framework/model as per relevant industry best practices, global standards, and regulations like CSA CCM, COBIT 5, NIST RMF, ISO/IEC 27017, HIPAA, PCI-DSS, EU GDPR, etc.

Understand how a contract impacts your governance framework/model.

- Obtain and review contracts (and any referenced documents) before entering into an agreement.
- Don't assume that you can effectively negotiate contracts with a cloud provider—but this also shouldn't necessarily stop you from using that provider.
- If a contract can't be effectively negotiated and you perceive an unacceptable risk, consider alternate mechanisms to manage that risk (e.g., monitoring or encryption).

135

Governance & Risk Recommendations

Develop a process for cloud provider assessments.

This should include:

- Contract review.
- Self-reported compliance review.
- Documentation and policies.
- Available audits and assessments.
- Service reviews adapting to the customer's requirements.
- Strong change-management policies to monitor changes in the organization's use of the cloud services.

Cloud provider re-assessments should occur on a scheduled basis and be automated if possible.

136

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Governance & Risk Recommendations

Cloud providers should offer easy access to documentation and reports needed by cloud prospects for assessments.

- For example, the CSA STAR registry.

Align risk requirements to the specific assets involved and the risk tolerance for those assets.

Create a specific risk management and risk acceptance/mitigation methodology to assess the risks of every solution in the space

Use controls to manage residual risks.

- If residual risks remain, choose to accept or avoid the risks.

Use tooling to track approved providers based on asset type (e.g., linked to data classification), cloud usage, and management.

cloud security alliance®

137

INSTRUCTOR LOGO HERE
Change img on all slide masters.

137

Review

1. Enterprise risk management includes all-risk management for the entire organization.
2. Information risk management focuses on the risk to information and must still align with the risk tolerance of the data owner.
3. The effort in a risk assessment should align with the value of the data. Just because something is moving to the cloud doesn't mean you now need to treat it as being higher-value.
4. In terms of risk, like security, IaaS is most closely aligned to traditional infrastructure, while with SaaS there is a greater reliance on the cloud provider.
5. Private cloud risks may be similar to that of public cloud if the private cloud is hosted and/or managed by a third party.

cloud security alliance®

138

INSTRUCTOR LOGO HERE
Change img on all slide masters.

138

Copyright 2019 Cloud Security Alliance and Securosis, LLC

139

Compliance

Obligations arise from multiple sources

- Legislation
- Broad based regulation
- Industry specific regulation
- Contracts

Compliance and Audits

- Compliance validates awareness of and adherence to corporate obligations
- Audits are a key tool for proving (or disproving) compliance.

CSA cloud security alliance®

140

INSTRUCTOR LOGO HERE
Change img on all slide masters.

140

Copyright 2019 Cloud Security Alliance and Securosis, LLC

HOW Cloud Changes Compliance

- The cloud customer is always responsible for compliance but may now also rely on the provider.
- Cloud customers will rely more on third-party assessments.
- The cloud metastructure may span jurisdictions, while the data/assets don't; this must be integrated into compliance activities.
- Not all cloud providers are equal with regards to compliance, and not all services from a single provider are always within the same audit / attestation / certification scope.

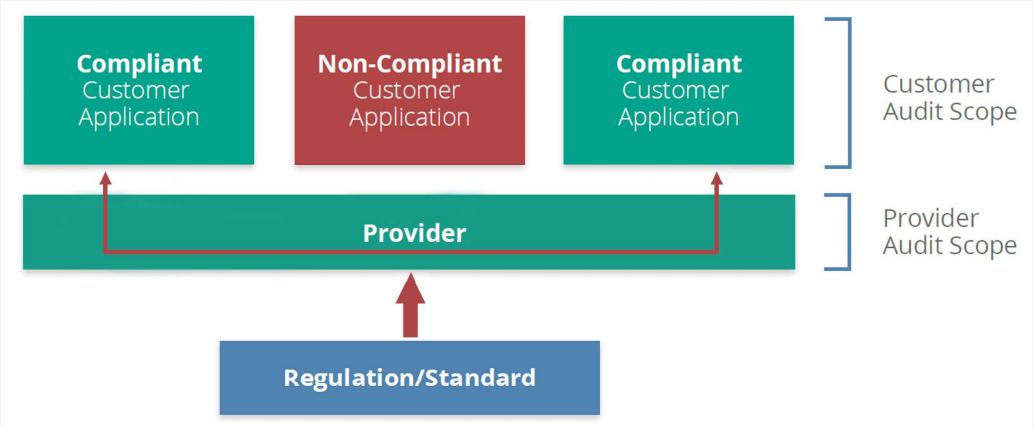
CSA cloud security alliance®

141

INSTRUCTOR LOGO HERE
Change Img on all slide masters.

141

Compliance Inheritance



CSA cloud security alliance®

142

INSTRUCTOR LOGO HERE
Change Img on all slide masters.

142

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Recommendations

Compliance, audit, and assurance should be continuous.

- They should not be seen as merely point-in-time activities, and many standards and regulations are moving more towards this model. This is especially true in cloud computing, where both the provider & customer tend to be in more constant flux and are rarely ever in a static state.

Cloud providers should clearly communicate their audit results, certifications and attestations, with particular attention to:

- The scope of assessments.
- Which specific features/services are covered in which locations and jurisdictions.
- How customers can deploy compliant applications and services on the cloud
- Any additional customer responsibilities and limitations.

Cloud providers must maintain their certifications/attestations over time and proactively communicate any changes in status

Cloud providers should engage in continuous compliance initiatives to avoid creating any gaps, and thus exposures, for their customers.

Provide customers commonly needed evidence and artifacts of compliance, such as logs of administrative activity the customer cannot otherwise collect on their own.

CSA cloud security alliance®

143

INSTRUCTOR LOGO HERE
Change img on all slide masters.

143

Recommendations

Cloud customers should:

- Understand their full compliance obligations before deploying, migrating to or developing in the cloud.
- Evaluate a provider's 3rd-party attestations and certifications and align those to compliance needs.
- Understand the scope of assessments and certifications, including both the controls and the features/services covered.
- Ensure they understand what artifacts of compliance the provider offers.
- Effectively collect and manage provider offered artifacts.
- Create and collect their own artifacts when the provider's artifacts are not sufficient.

Keep a register of cloud providers used, relevant requirements and current status. The CSA Cloud Controls Matrix can support this activity.

CSA cloud security alliance®

144

INSTRUCTOR LOGO HERE
Change img on all slide masters.

144

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Review

1. Compliance is a tool to ensure organizations are meeting corporate obligations.
2. Audits are how we validate compliance, and they can be performed internally or externally using third parties.
3. Cloud changes compliance because it now becomes a shared responsibility between the cloud consumer and the provider.
4. Compliance inheritance is the principle that if a cloud provider's service is compliant with a regulation/standard, then cloud consumers can build compliant services/applications using that service. But it does not guarantee compliance since the cloud consumer can still build a non-compliant application on top of a compliant service.

cloud security alliance

145

INSTRUCTOR LOGO HERE
Change img on all slide masters.

145

146

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Representative Laws & Implementing Regulations

- Is the applicable law where your business resides, where the data resides, or where the customer resides?
- Privacy regulations tend to be the most impactful on cloud security operations
- Don't worry, these are here as background and you don't need to memorize these regulations.

CSA cloud security alliance®

147

INSTRUCTOR LOGO HERE
Change img on all slide masters.

147

Asia Pacific (APAC) // Australia

- Privacy Act of 1988
  - 13 Australian Privacy Principles (APPs)
  - Applies to private, not-for-profits with 3+ million AUD, private healthcare providers
- Australian Consumer Law (ACL)

CSA cloud security alliance®

148

INSTRUCTOR LOGO HERE
Change img on all slide masters.

148

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Asia Pacific (APAC) // Australia

- Entities must provide notification when breaches occur
- ACL protects against false/misleading contracts and failed breach notifications
- Privacy Act applies to Australian customers even if CSP is based elsewhere

CSA cloud security alliance®

149

INSTRUCTOR LOGO HERE
Change img on all slide masters.

149

China

- 2017 Cyber Security Law governs network operators
  - Data localization requires certain data is stored in the country
- Privacy landscape still in transition

CSA cloud security alliance®

150

INSTRUCTOR LOGO HERE
Change img on all slide masters.

150

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Japan

- Act on the Protection of Personal Information (APPI) requires private sector to protect personal information
- Prior consent required for data transferred to 3rd party outside the country
- Consent is not required if certain standards are met as outlined by the Personal Information Protection Commission

CSA cloud security alliance®

151

INSTRUCTOR LOGO HERE
Change img on all slide masters.

151

Russia

- Russian data protection laws require consent for most data processing
- Companies are required to store personal data of Russian citizens within Russia

CSA cloud security alliance®

152

INSTRUCTOR LOGO HERE
Change img on all slide masters.

152

Copyright 2019 Cloud Security Alliance and Securosis, LLC

EMEA // European Union & European Economic Area

- 2018 General Data Protection Regulation (GDPR)
- Member states can supplement the GDPR
- 2002 Directive on Privacy and Electronic Communications (new E-Privacy Regulation to replace it)

CSA cloud security alliance®

153

INSTRUCTOR LOGO HERE
Change img on all slide masters.

153

EMEA // European Union & European Economic Area

- Network Information Security Directive (NIS Directive)
- Protects critical infrastructure and essential services

CSA cloud security alliance®

154

INSTRUCTOR LOGO HERE
Change img on all slide masters.

154

Copyright 2019 Cloud Security Alliance and Securosis, LLC

General Data Protection Regulation (GDPR)

Applicability

- Applies to data controllers/ processors in the EU/EEA, or activities within and outside the EU/EEA
- Applies to controllers/ processors outside the EU/EEA if monitoring or processing data owned by an individual in the EU/EEA

Accountability Obligations

- Entities must keep records of data processing activities
- Must develop and operate according to "privacy by design" and "privacy by default" principles

155

General Data Protection Regulation (GDPR)

Data Subjects' Rights

- Subjects have a right to know what info an entity has about them
- Right to object to how personal data is used
- Right to data erasure/corrections
- Right to be forgotten

Cross-Border Data Transfer Restrictions

- Personal data cannot transfer across borders unless a country has similar data and privacy rights.
- Entities outside of the EU/EEA must show an adequate level of protection

156

Copyright 2019 Cloud Security Alliance and Securosis, LLC

General Data Protection Regulation (GDPR)

Breaches of Security

- Entities must report a security breach to the Supervisory Authority or Authorities and data subjects when the breach meets certain thresholds.

Sanctions

- Violators are subject to sanctions, up to 4% of global gross income, or up to EUR 20 million.

157

Network Information Security Directive (NIS)

- Requires that EU/EEA member states' laws govern network and information security requirements for digital and essential services: i.e., e-commerce, search engines, cloud computing.
- Providers outside the EU offering services inside the EU are accountable.
- Providers must notify agencies if an incident substantially impacts the provision of a service.

158

Copyright 2019 Cloud Security Alliance and Securosis, LLC

EMEA // Countries Outside EU/EEA

- Countries with similar protection laws to GDPR or 1995 EU Data Protection Directive: Dubai, Israel, Morocco, Senegal, South Africa, Qatar.

CSA cloud security alliance®

159

INSTRUCTOR LOGO HERE
Change img on all slide masters.

159

Central & South America

- Argentina, Chile, Colombia, Mexico, Peru and Uruguay have laws inspired mainly by the European directive 95/46/EC
- Many laws refer to the APEC Privacy Framework

CSA cloud security alliance®

160

INSTRUCTOR LOGO HERE
Change img on all slide masters.

160

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Canada

- Personal Information Protection and Electronic Documents Act (PIPEDA)
- Applies to entities subject to federal jurisdiction and all provincial jurisdictions

cloud security alliance®

161

INSTRUCTOR LOGO HERE
Change img on all slide masters.

161

United States

- No single national law for data protection and regulation.

cloud security alliance®

162

INSTRUCTOR LOGO HERE
Change img on all slide masters.

162

Copyright 2019 Cloud Security Alliance and Securosis, LLC

U.S. Federal Laws

- Among others, Gramm-Leach-Bliley Act (GLBA), Accountability Act of 1996 (HIPAA), Children's Online Privacy Protection Act of 1998 (COPPA) all regulate privacy and information security.
- Companies must adopt reasonable security measures around personal data.
- Organizations are responsible for subcontractors' actions.

CSA cloud security alliance®

163

INSTRUCTOR LOGO HERE
Change img on all slide masters.

163

U.S. State Laws

- State laws around data security apply to any entity that collects/processes data of an individual living in that state, regardless of where data is stored.
- Most state laws that address information security require a written contract between the entity and the service provider mandating use of reasonable security measures.

CSA cloud security alliance®

164

INSTRUCTOR LOGO HERE
Change img on all slide masters.

164

Copyright 2019 Cloud Security Alliance and Securosis, LLC

United States

Breaches of Security

- Private or gov't entities must notify individuals of security breaches.

Privacy Laws

- California Consumer Privacy Act (CCPA) protects data for individuals, families and devices. In effect Jan. 2020 – significant implications.

Federal & State Agencies

- Federal Trade Commission (FTC) & state attorneys general also enforce accountability in entities around privacy and security practices. These decrees give guidance around protection of personal information.

Industry Standards

- Created by private organizations, industry standards are not laws.
- Many industry standards related to the cloud are produced by these organizations on the right side of the screen.

OASIS Open standards. Open source.
ETSI
IEEE
ISO
IEC
ITU
NIST National Institute of Standards and Technology U.S. Department of Commerce

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Contracts

Before Entering Negotiations

- Due diligence of your own entity
- Due diligence of other party
  - Does the service allow your company to meet its objectives & still be in compliance?

Contract Terms

- Pricing
- Allocation of Risk/Responsibility
- Termination
- Representation and Warranties
- Data/IP Ownership
- Data Location
- SLA
- Privacy/Privacy Level Agreement (PLA)

167

Contracts

During Performance

- Monitoring
- Preparing for termination and transition
- Unintended contract
- Closing

168

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Review

Due to the nature of the cloud, it has become easy to transfer data across the globe. However, the ease of movement of the data makes it susceptible to be caught under numerous legal systems. It is therefore important to appreciate the wide variety - as well as the amazing similarities - between the laws that govern cloud services.

In the past 10 years, the number of countries having privacy or security laws has more than doubled, and the number of laws that govern the privacy or security of company data and personal data has skyrocketed.

cloud security alliance®

GLOBAL TRENDS:

Protection of privacy and allowing individuals to have some control over the collection and use of their personal data.

There is a concern for the security of personal data and company data. A significant number of laws require the adoption of formal security policies

Countries and states are recognizing that security breach occurs for a variety of reasons - state actors, hackers, disgruntled employees, negligence or inadvertent error. These breaches should be notified to the affected parties. Numerous new laws require prompt disclosures to individuals and government agencies.

There is a concern that data laws many not be equivalent from state to state and countries are establishing barriers to prevent the transfer of data to those that do not offer "adequate protection".

Finally like for any other relationship, things are better recorded in writing. Contracts are important. Cloud contract can be tricky because it's easy to sign when they are just posted on a website for the customer to click on "I agree". Make sure you read them carefully to understand the terms.

169

INSTRUCTOR LOGO HERE
Change img on all slide masters.

169

170

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Audit

Different types of audit / assessment / attestation have different focuses and vary across providers.

Attestations are legal statements and providers may be required by the auditor to have an NDA with the customer before releasing.

Customers will likely be limited in their ability to assess (and vulnerability assess) providers. These could be a security risk to the provider.

Cloud providers should have a rigorous portfolio of compliance attestations to support their customers.

CSA cloud security alliance®

171

INSTRUCTOR LOGO HERE
Change img on all slide masters.

171

Previous Audit Results (3RD–Party Attestations)

Be aware of when the audit was performed, the scope of the audit, and the audit results.

CSA cloud security alliance®

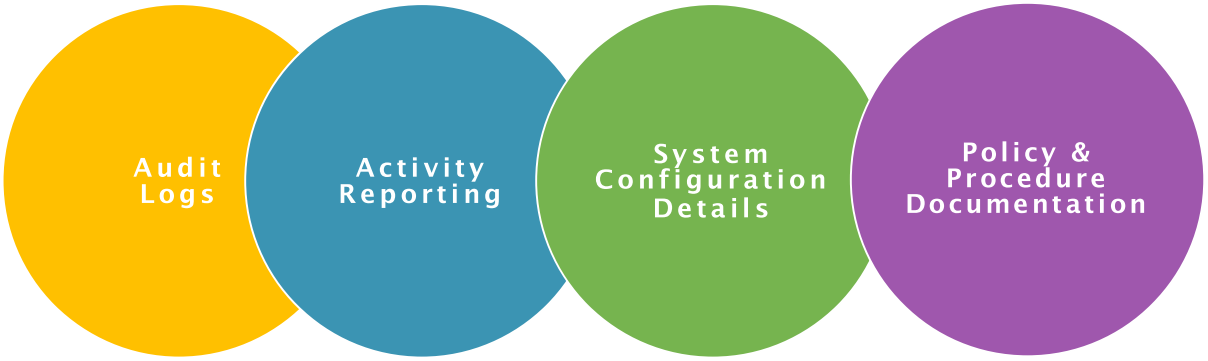
172

INSTRUCTOR LOGO HERE
Change img on all slide masters.

172

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Artifacts of Compliance



Need secure repositories and standards that may cross customer/provider boundary!

173

Artifacts of Compliance

- In cloud, assessing risk is collecting all audit evidence and can be challenging
- Understand requirements for logging and what kinds of data to collect
- Change in management logs are common artifacts you need.
- Map what you need to your cloud provider
- Collect admin activity to have logs of changes
- Store artifacts in a central repository
- Build architecture to store centrally

Key places to focus on:

- Management place
- Configuration pieces
- Adding more logging in applications
- System logs need to be pushed to a different location, ex: object storage on cloud provider

174

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Artifacts of Compliance

Core of audit considerations:

- Make sure you know what you need to collect to meet compliance obligations
- Evaluate what you can get from your cloud provider and how to get it
- Store in a central location
- Build in extra logging to compensate for places where you lose visibility

CSA cloud security alliance®

175

INSTRUCTOR LOGO HERE
Change img on all slide masters.

175

Assessment Frequency

Due to the evolving nature of a cloud service, more frequent assessment is required.

Consider STAR/CAIQ/CCM and other CSA tools and programs.

CCM CAIQ STAR

CSA cloud security alliance®

176

INSTRUCTOR LOGO HERE
Change img on all slide masters.

176

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Review

1. Different types of audits and assessments have different focuses, and even when the same name is used can have different focus and scope across cloud providers.
2. Cloud providers often limit the kinds of assessments their customers can use since some of these, like vulnerability assessments, can't be distinguished from real attacks without being constrained.
3. Ensure you know the scope, results, and timing (dates) of previous audits. Not all audits on a provider's website are necessarily up to date or cover the service under consideration.
4. Cloud consumers are responsible for maintaining their own artifacts of compliance for their own audits, such as log files.

CSA cloud security alliance®

177

INSTRUCTOR LOGO HERE
Change img on all slide masters.

177

CSA Tools

MODULE 3 // UNIT 7

178

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Cloud Controls Matrix

The CSA CCM is a controls framework for organizations to operate securely when cloud services are utilized.

- Intended for cloud providers, SaaS providers, other end-user services in the cloud
- Designed by SMEs across industries
- Provides security principles to providers to define and apply best practices
- Assists customers to assess cloud providers
- Standardized guidance on control objectives in cloud-based IT systems
- Based on CSA Security Guidance, research artifacts, Mobile WG
- Addresses intra- and inter-org challenges by delineating control ownership

179

Cloud Controls Matrix

The CSA CCM is a controls framework for organizations to operate securely when cloud services are utilized.

- Normalizes security expectations, cloud taxonomy, and security measures implemented in cloud supply chain
- Guides security efforts in vetting cloud providers, building proposal requests and operational risk assessment
- Aids in internal and external assessment and audits, and can submit to CSA STAR registry

180

Copyright 2019 Cloud Security Alliance and Securosis, LLC

CCMv3.0.1 CLOUD CONTROLS MATRIX VERSION 3.0.1

Control Domain	CCM V3.0 Control ID	Updated Control Specification	Architectural Relevance						Corp Gov Relevance	Cloud Service Delivery Model Applicability			Supplier Relationship					
			Phys	Network	Compute	Storage	App	Data		SaaS	PaaS	IaaS	Service Provider	Tenant / Consumer	COBIT 4.1	COBIT 5.0	COPPA	
Audit Assurance & Compliance Independent Audits	AAC-02	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.	X	X	X	X	X	X	X	X	X	X	X	X	DS5.5 ME2.5 ME 3.1 PO 9.6	APO12.04 APO12.05 DSS05.07 MEA02.06 MEA02.07 MEA02.08 MEA03.01	Title 16 Part 312	BOSS > Co Audits
Business Continuity Management & Operational Resilience Datacenter Utilities / Environmental Conditions	BCR-03	Data center utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.	X	X						X	X	X	X			DSS01.03 DSS01.04 DSS01.05	312.8 and	Infra Servic
Business Continuity Management & Operational Resilience Retention Policy	BCR-11	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.			X	X	X	X	X	X	X	X	X	X	DS 4.1 DS 4.2 DS 4.5 DS 4.9 DS 11.6	BAI09.01 BAI09.02 BAI09.03 DSS04.01 DSS04.02 DSS04.03 DSS04.04 DSS04.07 MEA03.01	312.3	BOSS > De Retention F
Change Control & Configuration Management Production Changes	CCC-05	Policies and procedures shall be established for managing the risks associated with applying changes to: • Business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations. • Infrastructure network and systems components. Technical measures shall be implemented to provide assurance that all changes directly correspond to a registered change request, business-critical or customer (tenant), and/or authorization by, the customer (tenant) as per agreement (SLA) prior to deployment.		X	X	X	X	X	X	X	X	X	X	X	A16.1 A17.6	BAI06.01 BAI06.02 BAI06.03 BAI06.04 BAI07.01 BAI07.03 BAI07.04 BAI07.05		ITOS > Se Managem

CSA CCM V3.0.1 | CCM Change Log

Ready

SAMPLE CCM

cloud security alliance®

181

INSTRUCTOR LOGO HERE
Change img on all slide masters.

181

Consensus Assessment Initiative Questionnaire

CAIQ

The CSA CAIQ assesses the security postures of a cloud service provider

- Originated in the CSA Consensus Assessment Initiative WG
- CAIQ is a simplified distillation of issues and control specs associated with cloud security
- Simple tools to standardize approach of validation of a cloud provider's security postures
- Companion to CSA Security Guidance and CCM
- Helps cloud SPs assess security postures, provides single location for details about their information security program
- Streamlines compliance assessments and improves communication between cloud SPs, business partners, and customers

cloud security alliance®

182

INSTRUCTOR LOGO HERE
Change img on all slide masters.

182

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Consensus Assessment Initiative Questionnaire

The CSA CAIQ assesses the security postures of a cloud service provider

- Allows customers and auditors to ask the right questions of cloud provider about their security posture.
- Consumers can use completed CAIQs to assess provider control and risk models
- Helps organizations build assessment processes prior and during to engagement with cloud provider.

183

Security, Trust, Assurance, & Risk Registry

Promotes security governance, assurance, and compliance in the cloud

- Based on CSA OCF, CCM, and CAIQ WGs
- Third-party resources that encompasses key principles of transparency, auditing, and standards harmonization
- Initially launched in 2010, STAR addresses lack of transparency in a burgeoning market
- Supports cloud customers in evaluation and selection process and helps cloud SPs to easily communicate security posture to their customers.
- Offers self-assessment, third-party certification, and continuous auditing
- Increases security by requesting adherence to best practices by implement CCM

184

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Security, Trust, Assurance, & Risk Registry

Promotes security governance, assurance, and compliance in the cloud

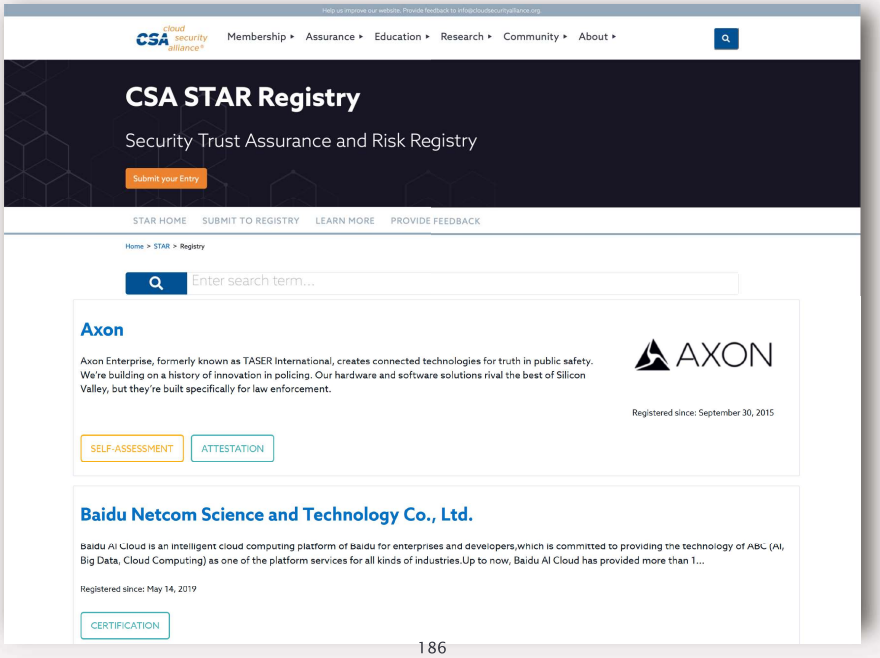
- Details security postures of security providers, offers assurance by indicating level of compliance of CSA best practices
- Offers layered approach to cloud assurance:
  - Self-assessment
  - Third-party certification and attestation
  - Continuous auditing
- Customer can access security documentation for cloud providers from a single trusted repository

CSA cloud security alliance®

185

INSTRUCTOR LOGO HERE
Change img on all slide masters.

185



CSA cloud security alliance®

186

INSTRUCTOR LOGO HERE
Change img on all slide masters.

186

Copyright 2019 Cloud Security Alliance and Securosis, LLC

STARWatch

The CSA STARWatch is a SaaS application to help cloud providers manage compliance with CSA STAR requirements

- STARWatch grew out of CSA's desires to manage CAIQ responses more effectively
- Facilitates adoption and implementation of CCM and CAIQ and streamlines provider and consumer compliance efforts
- Allows users to create, edit, import, and export CAIQs
- Intended for users of cloud services, cloud SPs, IT auditors, security solution providers and consultants
- Provides multi-user access to CCM and CAIQ in database format
- Incorporates a maturity model to measure the evolution of security posture of the org

187

STARWatch

The CSA STARWatch is a SaaS application to help cloud providers manage compliance with CSA STAR requirements

- Assistance in mapping security requirements to those of CSA
- Relevant mapping to relevant standards and regulations

188

Copyright 2019 Cloud Security Alliance and Securosis, LLC

Review

1. The Cloud Controls Matrix is a list of cloud security controls mapped by domain and aligned to various regulatory frameworks.
2. The CCM is an excellent tool for evaluating your cloud security controls and is useful to both cloud providers and consumers.
3. The Consensus Assessment Initiative Questionnaire is a standard set of security questions for cloud providers. It allows cloud consumers to directly compare providers and allows providers to reduce the need to respond to non-standard RFPs.
4. The Cloud Security Alliance Guidance (which this training is based on) tells you how to implement your controls, while the CCM tells you which controls to implement.
5. The STAR and StarWatch tool serve as central repositories and methods for cloud provider security documentation, including the CAIQ.

189

INSTRUCTOR LOGO HERE
Change img on all slide masters.

189

190

Copyright 2019 Cloud Security Alliance and Securosis, LLC