TOOLS and BEST PRACTICES

Daniele Catteddu
Managing Director EMEA,
Cloud Security Alliance
“To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing.”

• Global, not-for-profit organization
• Over 65,000 individual members, more than 200 corporate members, and 65 chapters
• Building best practices and a trusted cloud ecosystem
  • Agile philosophy, rapid development of applied research
  • GRC: Balance compliance with risk management
  • Reference models: build using existing standards
  • Identity: a key foundation of a functioning cloud economy
  • Champion interoperability
  • Enable innovation
  • Advocacy of prudent public policy
ABOUT THE CLOUD SECURITY ALLIANCE

“To promote the use of best practices for providing security assurance within Cloud Computing, and provide education on the uses of Cloud Computing to help secure all other forms of computing.”

• RESEARCH
  • https://cloudsecurityalliance.org/research/

• ADVISE GOVERNMENTS AND PRIVATE COMPANIES

• EDUCATION – PROFESSIONAL CERTIFICATION – TRAINING
  • https://cloudsecurityalliance.org/education/

• PROVIDER CERTIFICATION
  • https://cloudsecurityalliance.org/star/

• STANDARDS
  • https://cloudsecurityalliance.org/isc/

• Events
  • https://cloudsecurityalliance.org/events/
AGENDA

- GRC STACK
- CCM & CAIQ
- OCF / STAR
- Privacy Level Agreement
THE “BIG ROCKS” OF CLOUD SECURITY, TRUST, AND CONTROL

Take care of the big rocks first…
KEY CLOUD SECURITY PROBLEMS

FROM CSA TOP THREATS RESEARCH

• Trust: Lack of Provider transparency, impacts Governance, Risk Management, Compliance, and the capture of real value
• Data: Leakage, Loss or Storage in unfriendly geography
• Insecure Cloud software
• Malicious use of Cloud services
• Account/Service Hijacking
• Malicious Insiders
• Cloud-specific attacks

© Cloud Security Alliance, 2014.
THE ROOTS OF THE VALUE EQUATION IN THE CLOUD

IMPACT

• Information risk management transition & transformation planning
  • Policy
  • Governance
  • Compliance & Risk Management Thresholds

• Business model
• Downstream application of reclaimed transparency

© Cloud Security Alliance, 2014.
CSA GRC Stack
THE GRC STACK
Solving the Value Equation in the Cloud

GRC Stack

Needs and Claims
- Security Requirements and Capabilities

Evidence and Assurance
- Security Transparency and Visibility

Payoffs and Protection
- Compliance and Trust

VALUE Captured
Delivering evidence-based confidence... with compliance-supporting data & artifacts.

© Cloud Security Alliance, 2014.
THE CSA GRC STACK

• A suite of four integrated and reinforcing CSA initiatives (the “stack packages”)
  • The Stack Packs
    • Cloud Controls Matrix
    • Consensus Assessments Initiative
    • Cloud Audit
    • CloudTrust Protocol

• Designed to support cloud consumers and cloud providers
• Prepared to capture value from the cloud as well as support compliance and control within the cloud
## A COMPLETE CLOUD SECURITY GOVERNANCE, RISK, AND COMPLIANCE (GRC) STACK

<table>
<thead>
<tr>
<th>Delivering</th>
<th>Stack Pack</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Continuous monitoring ... with a purpose</td>
<td>CTP™</td>
<td>• Common technique and nomenclature to request and receive evidence and affirmation of current cloud service operating circumstances from cloud providers</td>
</tr>
<tr>
<td>Claims, offers, and the basis for auditing service delivery</td>
<td>Cloud Audit™</td>
<td>• Common interface and namespace to automate the Audit, Assertion, Assessment, and Assurance (A6) of cloud environments</td>
</tr>
<tr>
<td>Pre-audit checklists and questionnaires to inventory controls</td>
<td>CAI™</td>
<td>• Industry-accepted ways to document what security controls exist</td>
</tr>
<tr>
<td>The recommended foundations for controls</td>
<td>CCM™</td>
<td>• Fundamental security principles in specifying the overall security needs of a cloud consumers and assessing the overall security risk of a cloud provider</td>
</tr>
</tbody>
</table>

© Cloud Security Alliance, 2014.
What control requirements should I have as a cloud consumer or cloud provider?

How do I ask about the control requirements that are satisfied (consumer) or express my claim of control response (provider)?

How do I announce and automate my claims of audit support for all of the various compliance mandates and control obligations?

How do I know that the controls I need are working for me now (consumer)? How do I provide actual security and transparency of service to all of my cloud users (provider)?
CLOUD CONTROL MATRIX (CCM)

CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE (CAIQ)

© Cloud Security Alliance, 2014.
WHAT IS THE CCM?

• First ever baseline control framework specifically designed for Cloud supply chain risk management:
  • Delineates control ownership (Provider, Customer)
  • An anchor for security and compliance posture measurement
  • Provides a framework of 16 control domains
  • Controls map to global regulations and security standards

• Industry Driven Effort: 120+ Peer Review Participants

• Backbone of the Open Certification Framework and STAR
CCM V3.0.1 – 16 CONTROL AREAS

- AIS Application & Interface Security
- AAC Audit Assurance & Compliance
- BCR Business Continuity Mgmt & Op Resilience
- CCC Change Control & Configuration Management
- DSI Data Security & Information Lifecycle Mgmt
- DSC Datacenter Security
- EKM Encryption & Key Management
- GRM Governance & Risk Management

- HRS Human Resources Security
- IAM Identity & Access Management
- IVS Infrastructure & Virtualization
- IPY Interoperability & Portability
- MOS Mobile Security
- SEF Sec. Incident Mgmt, E-Disc & Cloud Forensics
- STA Supply Chain Mgmt, Transparency & Accountability
- TVM Threat & Vulnerability Management

136 CONTROLS
Cloud Controls Matrix v3.0

133 CONTROLS
Cloud Controls Matrix v3.0.1

© Cloud Security Alliance, 2014.
CCM v3.0.1

Current Version: Released July 10, 2014

• Builds upon the 5 new domains introduced in v3.0
  • Mobile Security
  • Supply Chain Management
  • Transparency & Accountability; Interoperability & Portability
  • Encryption & Key Management

• Continued improvements in controls including:
  • Language and auditability
  • Reduction of overlapping controls
  • Removed Customer and Provider references within the language

© Cloud Security Alliance, 2014.
CCM v3.0.1

- New and Updated Mappings including:
  - AICPA 2014 TSC
  - ISO/IEC 27001-2013
  - PCI DSS v3.0
  - NIST SP800-53 R3 App J
  - ENISA IAF
  - 95/46/EC - European Union Data Protection Directive
  - HIPAA / HITECH Act
  - COBIT 5.0
  - Canada PIPEDA
  - COPPA
  - ODCA UM: PA R2.0
CAIQ v3.0.1

Current Version: Released July 10, 2014

• Companion to CSA CCM v3.0.1 and aligned to CSA’s Guidance

• Questions mapped to the compliance requirements in CCM v3.0.1

• Helps organizations build assessment processes for cloud providers

• Helps cloud providers assess their own security posture

• Improved cohesion between CCM and CAIQ in v3.0.1

• Questions updated to facilitate STAR measurement

© Cloud Security Alliance, 2014.
## ALIGNMENT CCM & CAIQ

<table>
<thead>
<tr>
<th>Control Group</th>
<th>CGID</th>
<th>CID</th>
<th>Control Specification</th>
<th>Consensus Assessment Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Continuity Management &amp; Operational Resilience Equipment Maintenance</td>
<td>BCR-07</td>
<td>BCR-07.1</td>
<td>Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.</td>
<td>If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BCR-07.2</td>
<td></td>
<td>If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BCR-07.3</td>
<td></td>
<td>If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BCR-07.4</td>
<td></td>
<td>If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own offsite storage location?</td>
</tr>
<tr>
<td></td>
<td></td>
<td>BCR-07.5</td>
<td></td>
<td>Does your cloud solution include software/provider independent restore and recovery?</td>
</tr>
</tbody>
</table>

Controls now directly referenced

Numbering & questions linked to control

© Cloud Security Alliance, 2014.
FUTURE OF CCM

• Continue to improve controls:
  • Auditability & Measurement
  • Clarity
  • Intent
• Revisit the development cycle
• Evaluate additional candidates for mapping
OPEN CERTIFICATION FRAMEWORK (OCF)
CLOUD BARRIERS

• (Perceived) Loss of control
• Lack of clarity around the definition and attribution of responsibilities and liabilities
• Difficulties achieving accountability across the cloud supply chain
• Incoherent global (and even sometimes regional and national) legal framework and compliance regimes
....AND MORE BARRIERS

• The lack of transparency of some service providers or brokers
• Lack of clarity in Service Level Agreements
• Lack of interoperability.
• Lack of awareness and expertise
Launched in 2011, the CSA STAR is the first step in improving transparency and assurance in the cloud. The STAR is a publicly accessible registry that documents the security controls provided by cloud computing offerings. It helps users to assess the security of cloud providers. It is based on a multilayered structure defined by the Open Certification Framework Working Group.
The CSA Open Certification Framework is an industry initiative to allow global, accredited, trusted certification of cloud providers.
The CSA Open Certification Framework is an industry initiative to allow global, accredited, trusted certification of cloud providers.
• Self Assessments based on Consensus Assessments Initiative Questionnaire and Cloud Control Matrix
• Voluntary industry action promoting transparency
• Open to ALL cloud providers
• Since the initial launch at the end of had tremendous growth
• 59 entries: including Amazon Web Services, Box.com, HP, Microsoft, Ping Identity, Red Hat, Symantec, Terremark and many others

© Cloud Security Alliance, 2014.
The CSA Open Certification Framework is an industry initiative to allow global, accredited, trusted certification of cloud providers.

© Cloud Security Alliance, 2014.
The CSA Open Certification Framework is an industry initiative to allow global, accredited, trusted certification of cloud providers.
• CSA STAR Continuous will be based on a continuous auditing/assessment of relevant security properties.

• It will be built on the following CSA best practices/standards:
  • Cloud Control Matrix (CCM)
  • Cloud Trust Protocol (CTP)
  • CloudAudit (A6)

• CSA STAR Continuous is currently under development and the target date of delivery is 2015.
The CSA Open Certification Framework is an industry initiative to allow global, accredited, trusted certification of cloud providers.

© Cloud Security Alliance, 2014.
WHAT IS CSA STAR CERTIFICATION?
WHAT IS CSA STAR CERTIFICATION?

• The CSA STAR Certification is a **rigorous third-party independent assessment** of the security of a cloud service provider.
• **Technology-neutral** certification leverages the requirements of the ISO/IEC 27001:2013 & the CSA CCM
• **Measures the capability levels** of the cloud service.
• Evaluates the efficiency of an organization’s ISMS and ensures the scope, processes and objectives are “**Fit for Purpose.**”
• Help organizations **prioritize areas for improvement** and lead them towards **business excellence**.
• Enables effective **comparison** across other organizations in the applicable sector.
• Based upon the **Plan, Do, Check, Act** (PDCA) approach
ASSESSING THE CCM – CONTROLS

<table>
<thead>
<tr>
<th>Clause</th>
<th>Sec</th>
<th>Control Objective/Control</th>
<th>Current Controls</th>
<th>Remarks or Justification</th>
<th>Selected Controls and Reasons for selection</th>
<th>Overview of implementation</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td></td>
<td>Information Security Policy</td>
<td>Existing controls</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.1.1</td>
<td></td>
<td>Information Security Policy Document</td>
<td>Existing controls</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5.1.2</td>
<td></td>
<td>Review of Information Security</td>
<td>Existing controls</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1</td>
<td></td>
<td>Internal Organization</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1.1</td>
<td></td>
<td>Management Commitment (security)</td>
<td>Existing controls</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1.2</td>
<td></td>
<td>Information Security Coordination</td>
<td>Existing controls</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1.3</td>
<td></td>
<td>Allocation of Information Security Responsibilities</td>
<td>Existing controls</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1.4</td>
<td></td>
<td>Authorization process for Information Processing facilities</td>
<td>Existing controls</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1.5</td>
<td></td>
<td>Confidentiality agreements</td>
<td>Existing controls</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1.6</td>
<td></td>
<td>Contact with authorities</td>
<td>Existing controls</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6.1.7</td>
<td></td>
<td>Contact with special interest groups</td>
<td>Existing controls</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Add controls to existing SOA

Additional CCM Controls

© Cloud Security Alliance, 2014.
MANAGEMENT CAPABILITY / MATURITY: SCORES

• When an Organization is audited a Management Capability Score will be assigned to each of the control areas in the CCM.
• This will indicate the capability of the management in this area to ensure the control is operating effectively.
• The management capability of the controls will be scored on a scale of 1-15. These scores have been divided into 5 different categories that describe the type of approach characteristic of each group of scores.

<table>
<thead>
<tr>
<th>Score</th>
<th>Descriptor</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-3</td>
<td>No Formal Approach</td>
</tr>
<tr>
<td>4-6</td>
<td>Reactive Approach</td>
</tr>
<tr>
<td>7-9</td>
<td>Proactive Approach</td>
</tr>
<tr>
<td>10-12</td>
<td>Improvement Based Approach</td>
</tr>
<tr>
<td>13-15</td>
<td>Optimising Approach</td>
</tr>
</tbody>
</table>
HOW TO TAKE THE JOURNEY

No Approach: The organization has an ad hoc and inconsistent approach to this privacy standard or practice.

Reactive: The organization has a consistent overall approach, but it is mostly undocumented.

Proactive: The organization has a documented, detailed approach, but no routine measurement or enforcement of it.

Improving: Process is characterized as a quantitatively managed process. A quantitatively managed process is a defined (capability level 3) process that is controlled using statistical and other quantitative techniques.

Innovating: Process that is improved based on an understanding of the common causes of variation inherent in the process.

© Cloud Security Alliance, 2014.
APPROVING ASSESSORS

• They must demonstrate knowledge of the Cloud Sector
  • Either through verifiable industry experience – this can include though assessing organizations
  • Or through completing CCSK certification or equivalent

• They must be a qualified auditor working a ISO 27006 accredited CB
  • Evidence of conducting ISO 27001 assessments for a certification body accredited by an IAF member to ISO 27006 or their qualifications as an auditor for that organization.

• They must complete the CSA approved course qualifying them to audit the CCM for STAR Certification (This course will be carried out by BSI)
STAR CERTIFICATION: CERTIFICATE
STAR CERTIFICATION: ENTRY

The information below is provided as a companion to the CSA STAR Certificate.

Client Name: HP Enterprise Cloud Services for Government (ECG-G)
Client URL: http://www.hp.com/enterprise/cloud
Client Description:

HP Enterprise Cloud Services for Government (ECS-G) is an ISO27001 certified Virtual Private Cloud (VPC) which is one of the first Cloud Services to gain the Cloud Security Alliance (CSA) Security, Trust and Assurance Registry (STAR) Certification within the UK. This service provides our Public Sector clients with desktop, infrastructure and networking without the high cost of owning and managing their own equipment or data centers. Designed and built for the enterprise, supporting high-end applications which can be quickly deployed in a secure, multi-tenant cloud environment, accessing the latest IT services without risk of developing such complex systems in-house. VPC enables self-provisioning to match your business needs as they change and evolve. HP’s proven hardware and software, together with its industry leading services, form one of the best and most secure converged cloud platforms to base your future ICT strategy upon.

Scope:

Information Security Management System for ECS-G Central Operations and Support Services. Security Operations Center, comprising managed security services, situational awareness, protective monitoring, and security incident management including the protection of customer data and company assets by the application of appropriate security controls.

This is in accordance with version 7.9.a of the regional states statement of applicability, and version 7.9.a of the Local Statement of Applicability. In association with ISO 27001 certification is 85256

CCA Version Used: 1.4
Certificate Expiry Date: 09/24/2016
Certificate Country: United Kingdom

Term of Certificate: 5 years
Certification Body: The British Standards Institution (BSI)
Certificate Number: STAR 600374
STAR ATTESTATION

OPEN CERTIFICATION FRAMEWORK

LEVEL 3
Continuous Monitoring-Based Certification

LEVEL 2
Third-Party Assessment-Based Certification

LEVEL 1
Self-Assessment

ASSURANCE

TRANSPARENCY

© Cloud Security Alliance, 2014.
STAR ATTESTATION

• Star Attestation is a program under Level 2 of the CSA STAR Program that provides a framework for CPAs performing independent assessments of cloud service providers using AICPA SOC 2(SM) engagements supplemented by criteria in the CSA Cloud Controls Matrix (CCM). This assessment:
  • Is based on a mature attest standard to improve trust in the cloud and in the Information and Communication Technology (ICT) market by offering transparency and assurance.
  • Allows for immediate adoption of the CCM as additional criteria and the flexibility to update the criteria as technology and market requirements change.
  • Does not require the use of any criteria that were not designed for, or readily accepted by cloud providers.
  • Provides for robust reporting on the suitability of the design and operating effectiveness of a service organization’s controls relevant to security and availability based on criteria in the AICPA’s Trust Services Principles and Criteria and the CCM.
SOC 2(SM) ENGAGEMENTS PROVIDE THE FOLLOWING KEY STRENGTHS FOR CONSIDERATION:

- Performed under AT 101, which is a mature AICPA attestation standard
- Provides for robust reporting on the service provider’s description of its system and on the service provider’s controls, including a description of the service auditor’s tests of controls
- Evaluation of controls over a period of time rather than a point in time
- Recognition with an AICPA Logo
NEXT STEPS

Pilot CloudTrust Protocol (CTP)

Integrate CTP in the Open Certification Framework (STAR Continuous)

Integrate Privacy Level Agreement into the Open Certification Framework

For more info on CSA Privacy Level Agreement results please check: https://cloudsecurityalliance.org/research/pla/
PRIVACY LEVEL AGREEMENT
Privacy Level Agreement

• Privacy Level Agreements (PLA) are intended to
  • Be used as an appendix to a Cloud Services Agreement
  • Describe the level of privacy protection that the CSP will provide to the customer

• Similar to Service Level Agreement (SLA) but focusing on privacy and data protection issues
Why a PLA?

• Provide a uniform structure
• Better, more complete, more relevant disclosures
• Consistency among companies’ disclosure
Content of PLA

- Contact information
- How data will be processed
- Unique issues
- Crossborder data transfer
- Security measures
- Security breach disclosure
- Data retention; data disposal
Privacy Contact Person

- Company name, address, place of establishment
- Local representative
- Data protection role in the relevant processing
  - Controller
  - Joint controller
  - Processor
  - Subprocessors
- Contact details of the Data Protection Officer, or privacy contact person to whom customer may address requests
How data will be processed

• Activities performed at the request and on behalf of the customer
  • Organization of data in database
  • Creation of reports
  • Ability to run searches or queries
  • Storage

• Activities performed at the initiative of the CSP
  • Decision to store the data in different countries
  • Decision to implement back-up or disaster recovery centers in different countries
  • Decision to respond to third party request for access
Specific data processing issues

Data location
Use of subcontractors
Installation of software on cloud customer’s system
Crossborder data transfers

• Whether the personal data would be transferred, backed-up, recovered, or accessible across borders
• What methods the CSP uses to address the restriction against the transfer of personal data out of the country or region
  • Adequacy decision
  • Model contract clauses
  • Binding corporate rules
  • (Safe Harbor)
Data security measures

• Identification of the security measures used to protect the personal data
  • Might be a reference to other disclosures regarding the company’s information security plan, processes and procedures
  • Might be a description of the security control frameworks followed by the company (e.g. ISO 27002, Enisa Information Assurance Framework, BITS Shared Assessment, CSA Cloud Controls Matrix)

• Customer’s ability to monitor / audit the CSP’s security practices regarding personal data protection
• Availability of third party audit
Security Breach Disclosure

• Whether the customer will be informed of data security breaches affecting the customer’s personal data that occurred on the CSP’s network or on the networks of the CSP’s service provider, subcontractors, hosting services
  • Within what time frame
  • How
DATA RETENTION, DISPOSAL

DATA PORTABILITY
• Whether and how the CSP will assist the customer in the potential migration of data to another provider

DATA RETENTION
• Duration of data retention

DATA DELETION
• Commitment to delete the personal data in a secure manner
THANK YOU!

CONTACT US

Daniele Catteddu; Managing Director
EMEA, Cloud Security Alliance

dcatteddu@cloudsecurityalliance.org
star-help@cloudsecurityalliance.org
https://cloudsecurityalliance.org/star/