Agenda

1. What problem are we solving?
2. Definitions (Attestation vs Certification)
3. Cloud Security Responsibilities and Risk Exposure
4. Who is responsible for cloud security?
5. Cloud Service Provider Certifications
6. CSA Open Certification Framework
7. Cumulus Project
8. Cloud Practitioner Certifications
9. Summary
What Problem are we Solving?

1. How do you know that the provider of your cloud services can be trusted with your .....?

2. What are you basing this trust on?

3. What level of assurance do you need?

4. How can you compare the security services provided by one cloud service provider with another?

5. How can you compare the security features of cloud service providers?

6. What needs to be included in service agreements and contracts?

7. How can you demonstrate competency in cloud security?
Definitions

Security Certification

• A statement by a recognized authority that a security evaluation has been undertaken competently and in accordance with appropriate regulations.

• The comprehensive assessment of the technical and non-technical security features and other safeguards of a system to establish the extent to which a particular system meets a set of specified security requirements for its use and environment.

Security Accreditation

• Formal declaration by a Designated Approval Authority (DAA) that an information system is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.

Attestation

• The act of showing or evidence showing that something is true.

• Involves having a third party organization review the practices of the service provider and make a statement about the security posture of the organization.
Certification vs Attestation

**Certification**
- Assessed against an externally governed framework and control standard.
- Assessed by a registrar from an accredited organization using a formal auditing standard.
- Common framework and collection of controls.
- Certification can be compared with other organizations.

**Attestation**
- Assessed against a framework and controls specific to the organization.
- Could be self-assessed or by an independent/qualified third party.
- From a service provider perspective, formal attestation reports such as a SOC 2 report may only be shared with existing customers.
- The assessment process is governed by standards but the object of the assessment is not.
- Attestations cannot be compared to other organizations.
Cloud security is a shared responsibility

Shared between the enterprise and the cloud provider, with varying responsibilities depending on the nature of the (X)aaS type

<table>
<thead>
<tr>
<th>Governance, Risk &amp; Compliance</th>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Platform Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Infrastructure Security</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Physical Security</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Private Cloud**: Full responsibility
- **IaaS**: Enterprise responsibility
- **PaaS**: Shared responsibility
- **SaaS**: Cloud provider responsibility
The nature of the CSP relationship determines the risk exposure

1. Risk Attributes
   • Financial stability
   • Geography
   • Capability / capacity / service-levels
   • Corporate strategy and leadership

2. Product / Service Profile
   • Type of service / implementation
   • Nature / extent of customer interaction
   • Access to intellectual property
   • Sensitivity to regulatory requirements

3. Level of Integration
   • Integration into end products
   • Emerging technologies, and alignment of technology and processes

4. Service Model affecting CSP Oversight
   • Staff augmentation
   • Managed service

Potential Risk Exposures

- Strategic / CSP Selection
- Information Security
- Reputation
- Transaction / Operational
- Financial
- Legal / Compliance
- Credit
- Contractual
- Geopolitical
- Business Continuity
Cloud Certification Considerations

Service Providers
- Ability to determine the level of security protection provided by the cloud service provider
- What are the legal implications?

Assurance Levels
- Level of certification to match the required level of assurance in the provision of the cloud services
- What is the right level of assurance?

Audit Requirements
- Obtain a 3rd party opinion based on accepted standards and practices
- Speciality audits for service providers

Professional Certifications
- Rely on the certified expertise of people involved in providing cloud services
- Obtain certifications to further a career
Cloud Service Provider Certifications

1. **Cloud Security Alliance (CSA) Security, Trust and Assurance Registry (STAR)**
   - Leading cloud security certifications based on the Open Certification Framework

   - Cloud certification using a baseline of security controls to support low and moderate impact systems based NIST 800-53 V4

3. **UK GCloud**
   - Assertion-based using implementation guidance in support of 14 cloud security principles

4. **TRUSTed Cloud Privacy Certification**
   - Review of data privacy management practices. If practices are consistent with the TRUSTe Privacy Program Requirements will be granted the TRUSTe Certified Privacy Seal

5. **Service Organizational Control (SOC) 2 compliance.**
   - SOC 2 certification is designed for a technology and cloud computing organizations. It provides the assurance that a service provider delivers secure, reliable and effective systems for information storage, com
Cloud Service Provider Certifications – continued

6. **ISO 27001 Certification**
   - Certification of the ISMS supporting the Cloud Services

7. **ISO/IEC 20000-7: Application of ISO/IEC 20000-1 to the cloud.**
   - Currently being developed.
   - To provide guidance on application of ISO/IEC 20000 Part 1 to the cloud.

8. **Hybrid Certification (externally certified and audited)**
   - Service Organization Controls 1 (SOC 1) Type II report
   - Service Organization Controls 2 (SOC 2) Type II report
   - ISO 27001 certification
   - PCI DSS Level 1
   - US Federal Risk and Authorization Management Program (FedRamp)
   - Audits including; ITAR, FIPS 140-2, FISMA/DIACAP, HIPAA ...
   - This approach is used by Amazon AWS, Rackspace and Microsoft Azure.

9. **CUMULUS - Certification infrastructure for Multi-Layer Cloud Services**
   - EU-based project for development of certification models, processes and tools

10. **Geography Specific**
    - Hong Kong/Guangdong cloud security assessment and certification scheme
    - Trusted Cloud Service Certification – China Cloud Computing Promotion and Policy Forum (CCCPPF)
Cloud Security Alliance (CSA) objective is to:

• Promote “best practices for providing security assurance within Cloud Computing”
• Inform consumers and providers on security issues
• Plays a role in addressing and implementing viable solutions for security challenges
• CSA will increase size and relevance as interest in implementing cloud solutions proliferate

The Benefits of CSA Certification include:

• Broad acceptance of the controls used for security;
• A juried certification process using globally accepted criteria (ISO 27001);
• Alignment with a broad selection of frameworks and criteria;
• Transparent and available information to support certifications; and
• Certification levels that are appropriate for the assurance required by the cloud service requirements.
The STAR approach offers 3 different levels of certification that would align with different levels of required assurance.

- The 1st level, CSA STAR Self-Assessment level, is obtained by registering the results of the Consensus Assessments Initiative Questionnaire (CAIQ) completed by the Cloud Service Provider.
- The 2nd level can be CSA STAR Certification, obtained from an independent assessment from an accredited 3rd party or CSA STAR Attestation, obtained from a conducted SOC 2 report using the AICPA Trust Service Criteria and the CSA CCM.
- The 3rd level, CSA STAR Continuous Monitoring is under development.

- Certification is built upon the globally accepted standard for information security management systems (ISO 27001).
The CCM provides a broad foundation to satisfy cloud security requirements. The CCM defines 133 controls under 16 domains. Each of the controls is cross-referenced with several other security frameworks including ISO 27001:2013, BITS, NIST 800-53 Revision 4, AICPA Trust Service Criteria and PCI DSS V2 & V3 among others.
<table>
<thead>
<tr>
<th>Control Domain</th>
<th>CCM V3.0 Control ID</th>
<th>Updated Control Specification</th>
<th>ISO/IEC 27001-2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application &amp; Interface Security</td>
<td>AIS-01</td>
<td>Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.</td>
<td>A9.4.2, A9.4.1, A.14.2.3, 8.1*Partial, A.14.2.7, A.12.6.1, A.18.2.2</td>
</tr>
<tr>
<td>Audit Assurance &amp; Compliance</td>
<td>AAC-01</td>
<td>Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.</td>
<td>False Clauses 4.3(a), 4.3(b), 5.1(e), 5.1(f), 6.2(e), 9.1, 9.1(e), 9.2, 9.3(f), A.12.7.1</td>
</tr>
<tr>
<td>Change Control &amp; Configuration Management</td>
<td>CCC-01</td>
<td>Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or datacenter facilities have been pre-authorized by the organization’s business leadership or other accountable business role or function.</td>
<td>A.14.1.1, A.12.5.1, A.14.3.1, A.9.4.5, 8.1* (partial) A.14.2.7, A.18.1.3, A.18.1.4</td>
</tr>
<tr>
<td>Data Security &amp; Information Lifecycle Management</td>
<td>DSI-01</td>
<td>Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.</td>
<td>A.8.2.1</td>
</tr>
</tbody>
</table>
CSA – Cloud Assessments Initiative Questionnaire (CAIQ)

The CAIQ provides a tool that can be used to support the STAR self-assessment level of the Open Certification Framework

- It provides a set of questions a cloud consumer and cloud auditor may wish to ask of a cloud provider.
- It is a series of “yes or no” control assertion questions which can be tailored to suit each unique cloud customer’s requirements.
- There are 295 questions are based on the CSA Cloud Controls Matrix (CCM) using the same control groups and color coding.
- The questions are cross-referenced with other frameworks such as AICPA Trust Service Criteria, ISO 27001:2013, BITS, PIPEDA, COBIT, FedRamp, NIST 800-53, PCI DSS among others.
- The results of the questionnaire are contained in the STAR registry
<table>
<thead>
<tr>
<th>Control Group</th>
<th>CGI D</th>
<th>CID</th>
<th>Control Specification</th>
<th>Consensus Assessment Questions</th>
<th>CCM v3.0.1 Compliance Mapping</th>
</tr>
</thead>
</table>
| **Application & Interface Security**  
*Application Security* | AIS-01 | AIS-01.1 | Applications and programming interfaces (APIs) shall be designed, developed, deployed and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations. | Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)? | A9.4.2, A9.4.1, 8.1*Partial, A14.2.3, 8.1*partial, A14.2.7, A12.6.1, A18.2.2 |
| AIS-01.2 | | | | | |
| AIS-01.3 | | | | | |
| AIS-01.4 | | | | | |
| AIS-01.5 | | | | | |
| **Audit Assurance & Compliance**  
*Audit Planning* | AAC-01 | AAC-01.1 | Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits. | Do you produce audit assertions using a structured, industry accepted format (e.g., CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)? | Clauses 4.3(a), 4.3(b), 5.1(e), 5.1(f), 6.2(e), 9.1, 9.1(e), 9.2, 9.3(f), A12.7.1 |
CSA STAR Certification

- A STAR certification certificate cannot be issued unless the organization has passed their ISO 27001 assessment.

- The CSA maintains a registry of organizations that have completed one or more of the certification levels of the STAR certification framework.

- The STAR registry contains the information used for the CSA Open Certification Framework certifications.

- The self-assessment level will include the CSAQ self-assessment results.

- The certification level includes the STAR certification registry entry and may include the STAR certificate if.

- The attestation level includes the attestation from the 3rd party assessment organization.
Requirements for Bodies providing CSA STAR Certification

• A certification body conducting a CCM assessment must comply with ISO 27006.

• Accreditation is governed by ISO 27006:2011 *Requirements for bodies providing audit and certification for information security management systems* (the same standard for accrediting bodies for ISO 27001 certification).

• Assessors need to pass an accredited Lead Auditor Course for ISO 27001 or be a qualified and experienced ISO 27001 assessor for an International Accreditation Forum (IAF) member accredited ISO 27001 certification body.

• All assessors must have complete a BSI/CSA CCM exam.

• The scope of the ISO 27001 certification must not be less than the scope of the STAR certification.

• The assessment cycle is the same as ISO 27001 – initial assessment followed by surveillance audits over a 3-year period.
Certification infrastructure for Multi-Layer cloud Services

- The Cumulus project is a research project initiated by 8 partners from European science and industry to investigate how future cloud services can be made more secure and trustworthy.

- The problems that the Cumulus project is addressing:
  - There is difficulty to guarantee security properties of the different types of services available through clouds.
  - Service providers are reluctant to take full responsibility of the security of their services once the services are uploaded and offered through a cloud.
  - Cloud suppliers have historically refrained from accepting liability for a security leak.
  - The provision and security of a cloud service is sensitive to changes due to cloud operation.
Cumulus Project

The Cumulus project includes:

• “Development of advanced cloud service certification based on service testing data, service monitoring data and trusted computing platforms proofs”.

• Developing an integrated framework of models, processes and tools for certification at all layers of the cloud stack.

• Three initial industrial scenarios: eHealth, Smart Lighting and Smart Transportation.

• Development that is conducted under a number of development efforts organized as Work Packages.

1. WP 1 Project Management
2. WP 2 Certification Models and Processes
3. WP 3 Core Certification Mechanisms
4. WP 4 CUMULUS-aware Systems Engineering
5. WP 5 Infrastructure Design and Integration
6. WP 6 Industrial Scenarios and Validation
7. WP 7 Dissemination and Exploitation
Cumulus Certification – Work Package 2

- Certifying cloud-based applications and services.
- CUMULUS assumes that a certificate may be generated through a combination of three types of evidence (aka sources of trust):
  a) Test-based - test data regarding the component that is to be certified,
  b) Monitoring-based - monitoring data regarding the component that is to be certified, and/or
  c) Trusted computing based - other certificates that may have been generated for other properties of the component of interest or other components that contribute its implementation and which service provider depends on.
- Different certificate types are envisioned as the product of this project:
  - Test-based certificates
  - Hybrid certificates – combination of test-based and monitoring-based
  - Monitoring certificates
  - Dynamic certificates – combination of monitoring-based and trusted computing-based
  - Trusted computing-based certificates
- The design of these mechanisms will be informed by the Cumulus certification models and processes that will be developed in work package WP2.
Professional Cloud Security Certifications

1. **Cloud Security Alliance – Cloud Computing Knowledge Certification**

2. **Cloud Certification Council**
   - Provides professional certifications in specific areas of cloud computing

3. **Cloud U – Rackspace**
   - A vendor-neutral curriculum designed for IT professionals and business leaders that covers and certifies knowledge of the fundamentals of Cloud Computing

4. **CompTIA Cloud Essentials**
   - Covers the basic fundamentals of cloud computing and covers migration to the cloud and governance of cloud computing environments

5. **Cloud Certified Professional -- CloudSchool.com**
   - Offers a number of vendor-neutral cloud certifications aimed at competency in specific areas of cloud computing including Cloud Architects, Cloud Technology Professionals, Cloud Governance, and Cloud security, among others.
Professional Cloud Security Certifications

6. **IBM Certified Cloud Solution Architect v1 and v3**
   - demonstrate the design, plan, architecture and management capabilities for IBM's cloud computing infrastructure

7. **Google Certified Deployment Specialist**
   - covers the fundamental skills, knowledge and technical expertise required to deploy Google Apps for Business and Education

8. **Salesforce.com Certified Professional**
   - offers several certification tracks, including Salesforce Administrator, Force.com Developer, Implementation Expert, and Architect

9. **VMware Certified Professional**
   - offers six cloud-specific certifications, from beginner to advanced in a variety of cloud and virtualization-related technologies and methodologies.

10. **Red Hat Certificate of Expertise in Infrastructure-as-a-Service**
    - measures professionals' ability to design, build, deploy and manage private clouds based on the Red Hat Enterprise Linux OpenStack platform
Cloud Security Alliance Practitioner Certification

Certificate of Cloud Security Knowledge (CCSK)

• The CCSK certification is vendor-neutral, and certifies competency in key cloud security areas.
• Time-limited on-line exam of 60 multiple choice questions – pass is 80%
• The CSA offers CCSK Training

Security Guidance for Critical Areas of Focus in Cloud Computing V3

• 3 sections: Cloud Architecture, Governing the Cloud and Operating in the Cloud

14 Domains

2. Governance and Enterprise Risk Management
3. Legal Issues: Contracts and Electronic Discovery
4. Compliance and Audit Management
5. Information Management and Data Security
6. Interoperability and Portability
7. Traditional Security, Business Continuity and Disaster Recovery
8. Data Center Operations
9. Incident Response
10. Application Security
11. Encryption and Key Management
12. Identity, Entitlement and Access Management
13. Virtualization
14. Security as a Service
Cloud Credential Council Certifications

• The Cloud Credential Council (CCC) is a global provider of vendor-neutral cloud computing training and certification offering 9 certification programs.

• There are 5 professional level certifications, 2 associate level certifications.

• Training and a certificate of completion can be obtained for the US Federal FedRamp standard.

• Each certification focuses on a specific topic within the cloud computing space.

• The CCC provides training course and certification exams for each of the certification programs.

• CCC provided an opportunity to be grandfathered into a certification by proving existing experience and knowledge in Cloud Computing.
Cloud Credential Council (CCC)

**Professional Cloud Solutions Architect**
- designed for senior technology professionals who are architecting and designing the future generation of technology solutions

**Professional Cloud Security Manager**
- globally known as the standard of achievement for security and governance professionals involved with cloud-based solutions

**Professional Cloud Service Manager**
- Globally recognized certification for Service Management professionals

**Professional Cloud Administrator**
- demonstration of knowledge about Cloud Provisioning and Administration, Cloud Bursting, Interoperability, Strategic Policy Design, Disaster Recovery and Business Continuity, as well as Performance Measurement and Monitoring

**Professional Cloud Developer**
- Globally recognized certification for Developers of cloud solutions.

**Cloud Business Associate**
- demonstrates that candidates have the basic skill set and knowledge associated with cloud and business

**Cloud Technology Associate**
- demonstrates that candidates have the basic skill set and knowledge associated with cloud and virtualization

**Executive FedRamp Credential**
- Demonstrate a thorough understanding of aligning to FedRamp standard
Cloud School – Certified Cloud Professional (CCP)

- The Arcitura Cloud School offers a program of cloud professional certifications for several areas of cloud security specializations.

- The Cloud School provides vendor-neutral cloud computing training and certification offering 9 certifications.
  
  1. Certified Cloud Professional
  2. Certified Cloud Technology Professional
  3. Certified Cloud Architect
  4. Certified Cloud Security Specialist
  5. Certified Cloud Security Governance Specialist
  6. Certified Cloud Storage Specialist
  7. Certified Cloud Virtualization Specialist
  8. Certified Cloud Capacity Specialist
  9. Certified Cloud Trainer

- The Cloud School provides on-site training, public workshops and self-study programs

- There are 21 course modules covering specific cloud security topics offered in individual one-day courses.

- The certifications are based of 3 to 5 of the 21 modules.

- Exams are provided through Prometric testing centers.
## CCP Certification Matrix

| Exams | Certified Cloud Technology Professional | Certified Cloud Architect | Certified Cloud Security Specialist | Certified Cloud Governance Specialist | Certified Cloud Storage Specialist | Certified Cloud Virtualization Specialist | Certified Cloud Capacity Specialist *
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>C90.01: Fundamental Cloud Computing</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C90.02: Cloud Technology Concepts</td>
<td>x</td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C90.03: Cloud Technology Lab</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C90.04: Fundamental Cloud Architecture</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C90.05: Advanced Cloud Architecture</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C90.06: Cloud Architecture Lab</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C90.07: Fundamental Cloud Security</td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C90.08: Advanced Cloud Security</td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>C90.09: Cloud Security Lab</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>C90.10: Fundamental Cloud Governance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>C90.11: Advanced Cloud Governance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>C90.12: Cloud Governance Lab</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>C90.13: Fundamental Cloud Storage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>C90.14: Advanced Cloud Storage</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>C90.15: Cloud Storage Lab</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>C90.16: Fundamental Cloud Virtualization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>C90.17: Advanced Cloud Virtualization</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>C90.18: Cloud Virtualization Lab</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>C90.19: Fundamental Cloud Capacity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>C90.20: Advanced Cloud Capacity</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
<tr>
<td>C90.21: Cloud Capacity Lab</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>x</td>
</tr>
</tbody>
</table>
Summary

1. Determine what level of assurance is required
   - Is certification required or is self-assessment sufficient?
   - Do you need attestation to satisfy any regulatory requirements?

2. The CSA STAR certification has a high level of rigour and the potential for broad acceptance.
   - Based on ISO 27001 certification
   - The CSA CCM is aligned with most of the current security frameworks and requirements
   - The CCM provides a good framework for controls even if certification is not planned

3. There are lots of competency cloud security certifications to choose from
   - pick the one that will have the broadest recognition in your area of involvement.
   - Many professional certifications include training for the certification

4. The Cumulus project is very ambitious but will likely produce a broad set of results if the effort persists.