Cloud Security Standards:
A Comparison to assess Weaknesses and Suggest Improvements

Masooda Bashir, PhD
Assistant Professor School of Information Sciences
Carlo Di Giulio
Graduate Student
University of Illinois at Urbana Champaign
Cloud Computing means easy access to remote services, but also increased concern on security and privacy.

Certifications and compliance with standards are the easiest (if not only) indicator to evaluate a CSP from the outside.

To reassure users on the quality of services (IT and not), security standards are widely used by governments and industries.
2011 Federal Cloud Computing Strategy:

- Savings (The total IT expenditure in 2011 at a Federal level was $75.4 Billion)
- High security level in the cloud
- Creation of the Federal Risk Authorization Management Program (FedRAMP)
- Leveraging on NIST 800-53 requirements
FedRAMP and DISA Authorization

Impact level 5
FedRAMP Moderate + 47 controls
FedRAMP High + 12 controls (?)

Impact level (3) 4
FedRAMP High, or Moderate + 38 controls

Impact level 2
Same as FedRAMP Moderate baseline

Moderate Baseline
325 controls

Low Baseline
125 controls

• Only dedicated infrastructure
• Facility under the legal jurisdiction of the US
• Shared or dedicated infrastructure
• Within the US territory
• Other locations may be authorized according to mission requirements
• Shared or dedicated (not private cloud) infrastructure
• Location not specified
How a Control Looks Like

**AC-10 - Access Control - Concurrent Session Control**

The information system limits the number of concurrent sessions for each [Assignment: organization-defined account and/or account type] to [Assignment: organization-defined number]. (NIST SP 800-53)

**DSI-05 - Data Security & Information Lifecycle Management - Non-Production Data**

Production data shall not be replicated or used in non-production environments. (CSA CCM V. 3.0.1)

**A1.2 – Additional Criteria for Availability**

Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements. (AICPA TSC 2014)
FedRAMP is structured on 3 security tiers: low, moderate, and high.

The **low baseline** includes 125 controls and enhancements from NIST SP 800-53
The **moderate baseline** 325
The **high baseline** (released in July 2016) 421

There are equivalences between DoD authorization and FedRAMP:

- Level 2 = unclassified, non controlled information
- Level 4 = unclassified, controlled information (lower sensitivity)
- Level 5 = unclassified, controlled information (higher sensitivity)
- Level 6 = classified, secret to top secret
From a Vendor’s Point of View

10+ Standards, 
~1000 Control Requirements (CRs)

SOC 2 (5 Principles) – 116 CR 
Service Organization Controls
ISO 27001 – 26 CRs 
International Organization for Standardization
PCI DSS – 247 CRs 
Payment Card Industry – Data Security Standard
FedRAMP – 325 CRs 
Federal Risk and Authorization Management Program
ISO 27002 – 114 CRs 
International Organization for Standardization
SAFE HARBOR – 7 CRs 
Safe Harbor
SOX 404 (IT) – 63 CRs 
Sarbanes Oxley 404

~ 200 common controls across 11 control domains

Asset Management – 12 Controls
Access Control – 30 Controls
BCM – 10 Controls
Cryptography – 11 Controls
Data Privacy – 10 Controls
Incident Response – 6 Controls
Operations Management – 70 Controls
Physical and Env. Security – 16 Controls
People Resources – 11 Controls
SDLC – 11 Controls
Security Governance – 31 Controls

Additional resources: https://commoncontrolshub.com/
### FedRAMP (Moderate) and Others

<table>
<thead>
<tr>
<th>VENDORS</th>
<th>AUDITORS</th>
<th>COST</th>
</tr>
</thead>
<tbody>
<tr>
<td>#/compliant vendors in the US</td>
<td>Pre-requisites for Auditors</td>
<td>Initial cost for average company</td>
</tr>
<tr>
<td>• 73 (Sep 2016)</td>
<td>• ISO 17020 (Conformity assessment: inspections)</td>
<td>$250K +/- 85K (165-335K)*</td>
</tr>
<tr>
<td>• 664 (2014)</td>
<td>• ISO 17021 (Conformity assessment for auditors) • ISO 27006 (IT Security techniques for auditors)</td>
<td>$48K +/- 32K (16-80K)*</td>
</tr>
<tr>
<td>• N/A</td>
<td>• Certified Public Accountant</td>
<td>$55K +/- 15K (40-70K)*</td>
</tr>
</tbody>
</table>

*Information retrieved from www.pivotpointsecurity.com*
### ISO 27001 Certifications (and percentage variation)

<table>
<thead>
<tr>
<th>Year</th>
<th>2006</th>
<th>2007</th>
<th>2008</th>
<th>2009</th>
<th>2010</th>
<th>2011</th>
<th>2012</th>
<th>2013</th>
<th>2014</th>
</tr>
</thead>
<tbody>
<tr>
<td>Russian Federation*</td>
<td>5</td>
<td>9</td>
<td>17</td>
<td>53</td>
<td>72</td>
<td>31</td>
<td>27</td>
<td>48</td>
<td>50</td>
</tr>
<tr>
<td></td>
<td>44.44%</td>
<td>88.89%</td>
<td>211.76%</td>
<td>35.85%</td>
<td>-56.94%</td>
<td>-12.90%</td>
<td>77.78%</td>
<td>4.17%</td>
<td></td>
</tr>
<tr>
<td>Bulgaria</td>
<td>0</td>
<td>8</td>
<td>23</td>
<td>60</td>
<td>116</td>
<td>132</td>
<td>208</td>
<td>278</td>
<td>330</td>
</tr>
<tr>
<td></td>
<td>N/A</td>
<td>187.50%</td>
<td>160.87%</td>
<td>93.33%</td>
<td>13.79%</td>
<td>57.58%</td>
<td>33.65%</td>
<td>18.71%</td>
<td></td>
</tr>
<tr>
<td>Germany</td>
<td>95</td>
<td>135</td>
<td>239</td>
<td>253</td>
<td>357</td>
<td>424</td>
<td>488</td>
<td>581</td>
<td>640</td>
</tr>
<tr>
<td></td>
<td>29.63%</td>
<td>77.04%</td>
<td>5.86%</td>
<td>41.11%</td>
<td>18.77%</td>
<td>15.09%</td>
<td>19.06%</td>
<td>10.15%</td>
<td></td>
</tr>
<tr>
<td>USA</td>
<td>69</td>
<td>94</td>
<td>168</td>
<td>252</td>
<td>247</td>
<td>315</td>
<td>415</td>
<td>566</td>
<td>664</td>
</tr>
<tr>
<td></td>
<td>26.60%</td>
<td>78.72%</td>
<td>50.00%</td>
<td>-1.98%</td>
<td>27.53%</td>
<td>31.75%</td>
<td>36.39%</td>
<td>17.31%</td>
<td></td>
</tr>
<tr>
<td>Spain</td>
<td>23</td>
<td>93</td>
<td>203</td>
<td>483</td>
<td>711</td>
<td>642</td>
<td>805</td>
<td>799</td>
<td>701</td>
</tr>
<tr>
<td></td>
<td>75.27%</td>
<td>118.28%</td>
<td>137.93%</td>
<td>47.20%</td>
<td>-9.70%</td>
<td>25.39%</td>
<td>-0.75%</td>
<td>-12.27%</td>
<td></td>
</tr>
<tr>
<td>Taipei, Chinese</td>
<td>159</td>
<td>256</td>
<td>702</td>
<td>934</td>
<td>1028</td>
<td>791</td>
<td>855</td>
<td>918</td>
<td>781</td>
</tr>
<tr>
<td></td>
<td>37.89%</td>
<td>174.22%</td>
<td>33.05%</td>
<td>10.06%</td>
<td>-23.05%</td>
<td>8.09%</td>
<td>7.37%</td>
<td>-14.92%</td>
<td></td>
</tr>
<tr>
<td>Romania</td>
<td>4</td>
<td>16</td>
<td>44</td>
<td>303</td>
<td>350</td>
<td>575</td>
<td>866</td>
<td>840</td>
<td>893</td>
</tr>
<tr>
<td></td>
<td>75.00%</td>
<td>175.00%</td>
<td>588.64%</td>
<td>15.51%</td>
<td>64.29%</td>
<td>50.61%</td>
<td>-3.00%</td>
<td>6.31%</td>
<td></td>
</tr>
<tr>
<td>Italy</td>
<td>175</td>
<td>148</td>
<td>233</td>
<td>297</td>
<td>374</td>
<td>425</td>
<td>495</td>
<td>901</td>
<td>970</td>
</tr>
<tr>
<td></td>
<td>-18.24%</td>
<td>57.43%</td>
<td>27.47%</td>
<td>25.93%</td>
<td>13.64%</td>
<td>16.47%</td>
<td>82.02%</td>
<td>7.66%</td>
<td></td>
</tr>
<tr>
<td>China</td>
<td>75</td>
<td>146</td>
<td>236</td>
<td>459</td>
<td>957</td>
<td>1219</td>
<td>1490</td>
<td>1710</td>
<td>2002</td>
</tr>
<tr>
<td></td>
<td>48.63%</td>
<td>61.64%</td>
<td>94.49%</td>
<td>108.50%</td>
<td>27.38%</td>
<td>22.23%</td>
<td>14.77%</td>
<td>17.08%</td>
<td></td>
</tr>
<tr>
<td>India</td>
<td>369</td>
<td>508</td>
<td>813</td>
<td>1240</td>
<td>1281</td>
<td>1427</td>
<td>1611</td>
<td>1931</td>
<td>2170</td>
</tr>
<tr>
<td></td>
<td>27.36%</td>
<td>60.04%</td>
<td>52.52%</td>
<td>3.31%</td>
<td>11.40%</td>
<td>12.89%</td>
<td>19.86%</td>
<td>12.38%</td>
<td></td>
</tr>
<tr>
<td>United Kingdom</td>
<td>486</td>
<td>519</td>
<td>738</td>
<td>946</td>
<td>1157</td>
<td>1464</td>
<td>1701</td>
<td>1923</td>
<td>2261</td>
</tr>
<tr>
<td></td>
<td>6.36%</td>
<td>42.20%</td>
<td>28.18%</td>
<td>22.30%</td>
<td>26.53%</td>
<td>16.19%</td>
<td>13.05%</td>
<td>17.58%</td>
<td></td>
</tr>
<tr>
<td>Japan</td>
<td>3790</td>
<td>4896</td>
<td>4425</td>
<td>5508</td>
<td>6237</td>
<td>6914</td>
<td>7199</td>
<td>7140</td>
<td>7181</td>
</tr>
<tr>
<td></td>
<td>22.59%</td>
<td>-9.62%</td>
<td>24.47%</td>
<td>13.24%</td>
<td>10.85%</td>
<td>4.12%</td>
<td>-0.82%</td>
<td>0.57%</td>
<td></td>
</tr>
</tbody>
</table>
Gaps in the Literature

Industry/Non Academic Work

מנ STATES

Threats

Compliance

• Controls
• Adoption of current standards

Academic Work

Threats

Standards

• Outdated material
• Limited scope
• New approaches
Research Questions

- How effective are current IT security measures and frameworks at addressing cloud security?
- How do standards compare to each other?
- Is FedRAMP better than other security frameworks at protecting information assurance in cloud environments, and if so, how?
- Is it ultimately worth it to invest in new cloud security standards like FedRAMP?
- What can be done to improve current cloud security standards?
Analyzed Standards

- FedRAMP rev. 3 and 4. Moderate and High baseline (DoD Lev 2-4)
- BSI Cloud Computing Compliance Control Catalogue (C5)
Methodology

Collection and Classification of Security Controls

Analysis: Gaps and Differences

Analysis: Most Relevant Controls

RESULTS

In-Scope Frameworks

- BSI C5
- SOC 2 (TSPC)
- ISO/IEC 27001
- FedRAMP (Mod. Baseline)
- FedRAMP (High Baseline)

Supporting Material

- CSA CCM (133 controls, 16 domains)
- The Treacherous Twelve (issues in the cloud)
The CSA CCM and the T12

Step 1:
- Matching of guidelines
- Analysis of missing controls

Step 2
- Collection of Threats
- Matching on missing controls
The Treacherous Twelve (issues)

1. Data Breaches
2. Weak Identity, Credential and Access Management
3. Insecure APIs
4. System and Application Vulnerabilities
5. Account Hijacking
6. Malicious Insiders
7. Advanced Persistent Threats (APTs)
8. Data Loss
9. Insufficient Due Diligence
10. Abuse and Nefarious Use of Cloud Services
11. Denial of Service
12. Shared Technology Issues
Timeline and Missing Controls (CSA CCM)
Venn Diagram of Missing Controls

FedRAMP
- IAM-08
- DSI-02
- IVS-07
- IVS-05
- MOS

BSI C5
- SEF-04
- DCS-08
- BCR-10
- HRS-02
- HRS-10
- HRS-04

TSPC
- IPY
- IAM-10
- GRM-04
- GRM-08
- EKM-04
- IVS-11
- IVS-02
- IVS-13

ISO/IEC 27001
- IAM-01
Attack Tree (missing controls in CSA CCM)

Tenant Level
- Insider Threats
  - IAM-04
  - IAM-10

Virtualization Level
- Side Channels
  - DSI-02
  - IVS-13

- Vulnerabilities in the Virtualization Stack
  - IVS-05
  - IVS-07
  - SEF-04

Legend
- XXX-00: Missing in TSPC
- XXX-00: Missing in FedRAMP
- XXX-00: Missing in ISO
- XXX-00: Missing in C5
- No mitigations
- Mitigated by other measures

Cloud Level
- Misconfiguration (SaaS and PaaS)
  - IAM-01
  - IPY
  - EKM-04

- Insider Threats
  - IAM-08
  - MOS
  - IVS-02
  - IVS-11
  - GRM-04
  - GRM-08
  - DCS-08
  - HRS-02
  - HRS-10
  - BCR-10
  - HRS-04
What is "Cloud Computing?"

Alternate Attack Tree (SOC 2 excluded)

Legend:
- XXX-00: Missing in C5
- XXX-00: Missing in FedRAMP
- XXX-00: Missing in ISO
- ✗: No mitigations
- ✓: Mitigated by other measures

Cloud Level:
- Insider Threats
- Misconfiguration (SaaS and PaaS)
- Insufficient Due Diligence
- Improper Breach Management

Virtualization Level:
- Vulnerabilities in the Virtualization Stack
- Advanced Persistent Threats
- Side Channels

Legend:
- HRS-04: Missing in C5
- HRS-02: Missing in FedRAMP
- DCS-08: Missing in ISO
- BCR-10: No mitigations
- IVS-07: Mitigated by other measures
- IVS-05: No mitigations
- IVS-13: No mitigations
- HRS-10: Missing in C5
- MOS: Missing in FedRAMP
- IAM-01: Missing in ISO
- IAM-08: No mitigations
- IPY: Mitigated by other measures
- SEF-04: Mitigated by other measures
- DSI-02: No mitigations
Publications and Submissions


- International Workshop on Assured Cloud Computing And QoS Aware Big Data (WACC). Held in Conjunction with the 17th IEEE/ACM CCGRID. Madrid, Spain, May 14-17, 2017 (Submitted)

Conclusions

- Our analyses reveals that no standard is 100% secure.
- All standards that we examined has at least 2 serious omissions
  - For example, (ISO) or many more (e.g. SOC/TSPC and C5).
- Even if we obtain certification on more than 1 standard we cannot be sure of being protected either, since some standards omit the same controls (e.g. FedRAMP and SOC/TSPC).
- Although by combining all the standards higher security is achievable, a small effort is required to improve the response of one or few of them to current security threats.
Future Directions

- Insider threats are the greater risk to cloud assurance, and better measures to assure proper training to employees and raise their awareness is required.
- Expand the considerations on the impact of human factor on cloud security.
- Expand our research to the internet of things (IoT) and how the regulatory landscape is evolving to cope with new threats in IoT.
Thank You
Any Questions?

Prof. Masooda Bashir:
mnb@illinois.edu