Compliance in the Cloud: A Pragmatic Approach to SOC2 and PCI compliance
The Cadence Group is a professional services firm specializing in financial and IT compliance and risk management services. Our value proposition includes:

**Experience**
We don’t hire rookies, and are not in the business of providing on-the-job training. We only hire extremely experienced professionals.

**Flexibility**
Enabling clients to determine how to best use our expertise and experienced resources. We’re flexible and work with you to achieve the project goals.

**Efficiency**
Ensuring engagements are effectively managed and efficiently executed. Part of our job is to make sure you don’t do too much, or too little.
How did we all get HERE?
The Old School Approach

Build a data center on premise, hire DC operations people, build and/or buy applications deployed locally to racked breadbox servers

Big companies still (partially) operate in this manner
Then...

**SPECIALIZATION!**

(n): A method of production where a business or area focuses on the production of a limited scope of products or services in order to gain greater degrees of productive efficiency
Today’s Fast Company

Hire really smart people, give them a laptop, create apps, use cloud services

SaaS
PaaS
IaaS
SaaS – PaaS - IaaS

<table>
<thead>
<tr>
<th>Area of Responsibility</th>
<th>Type of Cloud Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data</td>
<td>IAAS</td>
</tr>
<tr>
<td>Software, user applications</td>
<td>PAAS</td>
</tr>
<tr>
<td>Operating systems, databases</td>
<td>SAAS</td>
</tr>
<tr>
<td>Virtual infrastructure (hypervisor, virtual appliances, VMs, virtual networks etc.)</td>
<td></td>
</tr>
<tr>
<td>Computer and network hardware (processor, memory, storage, cabling, etc.)</td>
<td></td>
</tr>
<tr>
<td>Data center (physical facility)</td>
<td></td>
</tr>
</tbody>
</table>

Customer Responsibility

Cloud Provider Responsibility

Compliance in the Cloud
How does this tie into Compliance?
Specifically SOC2 and PCI (and why do we do the Compliance Alphabet?)

SECURITY $\neq$ COMPLIANCE
What is the Catalyst for Beginning Compliance Initiatives?

Customer Demand?
Keeping up with the Jones’?
Just love compliance?
Data Breach?

By the way, anyone can (falsely) claim compliance on their website
Data BREACH
What is Pragmatic Compliance?

• Are these conflicting terms?
• Compliance does not have to be overwhelming
• Requires pragmatic advices and realistic planning
• Also requires buy-in from the top
What Compliance Framework / Program Should my Company Choose?

Compliance in the Cloud
Recently from the Cloud Security Alliance:

“After careful consideration of alternatives, the Cloud Security Alliance has determined that for most cloud providers, a SOC 2 Type 2 attestation examination conducted in accordance with AICPA standard AT Section 101 (AT 101) utilizing the CSA Cloud Controls Matrix (CCM) as additional suitable criteria is likely to meet the assurance and reporting needs of the majority of users of cloud services.”
What is SOC Reporting?

Service Organization Control (SOC) Reports are third party attestation report used by customers, prospective customers, and business partners to gain an understanding of the control environment at a service provider. Issued by a CPA firm with experience in SOC Reporting.

Various types of SOC reports:

- SOC1
- SOC2
- SOC3
- Type 1
- Type 2
### SOC Report Types

<table>
<thead>
<tr>
<th>SOC 1</th>
<th>SOC 2</th>
<th>SOC 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSAE16 – Service Auditor Guidance</td>
<td>AT 101</td>
<td>AT 101</td>
</tr>
<tr>
<td>Restricted Use Report (Type I or II report)</td>
<td>Generally a Restricted Use Report (Type I or II report)</td>
<td>General Use Report (with a public seal)</td>
</tr>
<tr>
<td>Purpose: Reports on Controls for Financial Statement Audits</td>
<td>Purpose: Reports on controls related to compliance or operations</td>
<td>Purpose: Reports on controls related to compliance or operations</td>
</tr>
</tbody>
</table>

**Trust Services Principles & Criteria**
**Type I**
Report of the design of the controls at a *point in time*. Are the controls designed and in place as of September 30, 2014? Typically utilized for first-time issuers, as a pre-cursor to the Type II report.

**Type II Report**
Report of the design *and operating effectiveness* of the controls over a specific period of time (minimum of six months, maximum of twelve months). A Type II report is what is expected by a service organization, and it’s auditors as the procedures are sufficient to replace the work they would otherwise have had to perform.
SOC2 Principles
Trust Services Principles and Criteria

Security  Availability  Confidentiality  Processing Integrity  Privacy
44        47          58           62                   73

A lot of redundancy and overlap
SOC2 Principles – New Common Criteria (CC)

Required for reports with audit periods ending after December 15, 2014 (can early adopt now)

Security
Availability (3)
Confidentiality (6)
Processing Integrity (6)
Privacy (still 73)

23 Common Criteria
Demystifying PCI

PCI = Payment Card Industry.

- Applies to anyone that transmits, processes, and/or stores cardholder data.
- Not a law.
PCI - Merchants

- Merchant level (1-4) based on annual transaction volume (not $$) by card brand.
- Level 1 (over 6m transactions / year / brand) requires an on-site PCI Assessment by a QSA.
- Levels 2-4 may complete a Self Assessment Questionnaire (SAQ)
  - 8 SAQ versions, depending on how cards are processed / stored
PCI - Service Providers

- Service Providers are entities that transmit, store, or process cardholder data on behalf of their customers.
- Compliance is driven more by customer demand, than by the card brands or banks (service providers are still fully liable in the event of a breach, not to mention the greater reputational risk).
- Much confusion / deception in the area of service provider PCI compliance.
<table>
<thead>
<tr>
<th><strong>DO:</strong></th>
<th><strong>DO NOT:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Maintain an accurate data flow diagram of where card data flows within your environment</td>
<td>1. Store Credit Card data if you don’t need it (evaluate why it is being kept at all).</td>
</tr>
<tr>
<td>2. Segment your network to minimize your PCI footprint</td>
<td>2. Ever store the security code (CVV2, etc.)</td>
</tr>
<tr>
<td>3. Encrypt Card holder data if it is stored</td>
<td>3. Assume that your employees are all benevolent angels that would never (intentionally or unintentionally) put customer data at risk of being stolen.</td>
</tr>
<tr>
<td>4. Consider outsourcing card processing and storage functions where possible</td>
<td>4. Forget that even when you outsource certain functions – the financial and reputational risk cannot be outsourced.</td>
</tr>
<tr>
<td>5. Create, distribute, and enforce policies related to general data security, and credit card handling procedures.</td>
<td>5. Assume that just because your encrypt data that all other security measures are unnecessary.</td>
</tr>
<tr>
<td>6. Maintain active/updated anti-virus and malware protection.</td>
<td>6. Forget to train employees on security-related topics.</td>
</tr>
<tr>
<td>7. Perform regular (at least quarterly) vulnerability scans and (at least annually) penetration tests</td>
<td>7. Use outdated software/OS systems</td>
</tr>
</tbody>
</table>
4 Steps for Pragmatic Compliance

What does this mean??
5 Steps for Pragmatic Compliance

1. Look at security as a sales tool, and consider the ROI
   These compliance steps are for big-boy companies, looking to land big enterprise customers – this is exciting! Security can be treated like insurance or a great sales tool (usually both).

2. Engage in compliance for reason with a clear goal
   Have clear goals in mind, with clear and realistic timelines (when does the audit need to occur?) Allow time for remediation.

3. Get executive buy-in
   Everything you do will be nothing more than a band-aid without executive buy-in.

4. Don’t create separate control matrices or projects for each compliance area
   Create an overall compliance program, then integrate the specific requirements of each area (SOC2, PCI, etc.) to take advantage of economies

5. Clearly identify the borders / scope of the project
   Create a spreadsheet that identifies the details of all systems, locations, and data elements in scope. Many of the compliance programs need only apply to specific areas of your environment.
Some Common SOC2 & PCI Roadblocks
Some Common SOC2 & PCI Roadblocks

1. Flat Networks
   Everything is connected and shared – great for business, not great for security

2. Lack of Access Control – especially at the DB level
   Open DB Access: Ultimately it is the data that needs protecting – why sneak in through the back door if the front door is wide open?
   Lack of SSO: Use SSO to encourage good password protection AND helps with BYOD.

3. BYOD (and it’s cousin – WOCD)
   How do you secure a device you don’t control? Use SSO to protect data, not device.

4. Anti-virus / Malware protection
   Ask Target and Home Depot how this works.

5. Lack of written policies and Security Awareness Training
   This also Helps with many other aspects of the business, and selling to large enterprise customers