CDSA’s App & Cloud Framework

May 27th 2020
TPN aims

- Improved content security in studio supply chain
- Common control set
- Efficient operations
- Shared audit reports for studios
- Reduced costs for vendors
- Global talent pool for auditors

New challenges

- Audience and revenues moving online
- Consolidation of digital production and distribution
- Rapid shift to cloud-based workflows
- New skills and security culture required
Content security

- **Evolution**
  - UK Broadcasters, Production, Vendors
  - US Studios
  - Common controls
  - Professional audit
  - Shared data across members

- **Controlled**
  - Checklist
  - Self certified
  - Oversight
  - Zero Trust

- **Regulated**
  - Legislation
  - Penalties

- **Guidance**
  - Awareness
  - Hygiene

- **Common controls**
  - Professional audit
  - Shared data across members

- **Regulated**
  - Legislation
  - Penalties
Security audit

- People & process
  - Facility
  - Asset management
  - Transport
- Digital
  - Infrastructure
  - Content management
  - Content transfer
- Cloud
  - Software release
App & cloud & integration

- Code
- Staff
- Partners
Complex software

- Amazon
- Netflix
- Google

https://www.slideshare.net/AmazonWebServices/releasing-missioncritical-softwar
Complex software

- Amazon
- Netflix
- Google
Shift to cloud

- It’s all about software
- New economics - CAPEX to OPEX
- Move the tools and skills to the work
- Frequency of audit

CDSA App & Cloud initiative launched to extend original programme to cover new use cases with a custom control set
Supply chain assurance

- Range of business sizes & types
- Effective security requires ongoing skills development
- Consistent approach depends on the weakest link in the chain
- Need to establish a security culture from CEO down
New approach

- Map controls from industry standards, with frequent updates
- Leverage cloud platforms best practice and design patterns
- Deliver documentation in a usable format that is easily applied to any size of business
- Automate tracking and checks to reduce the cost of audit
- Help develop new skills to build a security culture
1. Reduce controls maintenance effort
2. Leverage cloud platform collateral
3. Usable documentation, easy to adopt approach
4. Highlight control changes and new threats
5. Enable skills development
## Control set

<table>
<thead>
<tr>
<th>Index</th>
<th>CSAaD Mapping</th>
<th>Control Domain</th>
<th>Control Sub Domain</th>
<th>Updated Control Specification</th>
<th>Status</th>
<th>Control ID (CSAA Clue/DOAMA Pam)</th>
<th>Mapping Card File</th>
<th>Review comments</th>
<th>TNM/BNDD Section</th>
<th>TNM/BNDD Category Name</th>
<th>TNM/BNDD Control ID</th>
<th>Control Description</th>
<th>System Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Peasie &amp; privex</td>
<td>Audit Assurance &amp; Compliance</td>
<td>Independent Audits</td>
<td>Independent verifications and assessments shall be performed at least annually by a qualified assessor to ensure that the organization addresses new information technology policies, standards, procedures, and compliance gap analyses.</td>
<td>CMM 1.0.1</td>
<td>AAS-01</td>
<td>CMM 1.0.1</td>
<td>AAS-08</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>8</td>
<td>Peasie &amp; privex</td>
<td>Audit Assurance &amp; Compliance</td>
<td>Information System Regulatory Reporting</td>
<td>Organizations shall create and maintain a control framework which captures the regulations, laws, and statutes requirements relevant to their business needs. The control framework shall be updated at least annually to incorporate changes that could affect the business processes and requirements.</td>
<td>CMM 1.0.1</td>
<td>AAS-09</td>
<td>CMM 1.0.1</td>
<td>AAS-08</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>9</td>
<td>Peasie &amp; privex</td>
<td>Business Continuity Management &amp; Operational Excellence</td>
<td>Business Continuity Planning</td>
<td>Business Continuity Planning</td>
<td>CMM 1.0.1</td>
<td>BCP-01</td>
<td>CMM 1.0.1</td>
<td>BCP-01</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>10</td>
<td>Peasie &amp; privex</td>
<td>Business Continuity Management &amp; Operational Excellence</td>
<td>Business Continuity Planning</td>
<td>Business Continuity Planning</td>
<td>CMM 1.0.1</td>
<td>BCP-01</td>
<td>CMM 1.0.1</td>
<td>BCP-01</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>11</td>
<td>Peasie &amp; privex</td>
<td>Business Continuity Management &amp; Operational Excellence</td>
<td>Business Continuity Planning</td>
<td>Business Continuity Planning</td>
<td>CMM 1.0.1</td>
<td>BCP-01</td>
<td>CMM 1.0.1</td>
<td>BCP-01</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>12</td>
<td>Peasie &amp; privex</td>
<td>Business Continuity Management &amp; Operational Excellence</td>
<td>Disaster Recovery/ Business Resilience Conditions</td>
<td>Disaster Recovery/ Business Resilience Conditions</td>
<td>CMM 1.0.1</td>
<td>BCP-01</td>
<td>CMM 1.0.1</td>
<td>BCP-01</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>13</td>
<td>Peasie &amp; privex</td>
<td>Business Continuity Management &amp; Operational Excellence</td>
<td>Documentation</td>
<td>Information systems documentation (e.g., administrative and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following:</td>
<td>CMM 1.0.1</td>
<td>BCP-01</td>
<td>CMM 1.0.1</td>
<td>BCP-01</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>14</td>
<td>Peasie &amp; privex</td>
<td>Business Continuity Management &amp; Operational Excellence</td>
<td>Environmental Rules</td>
<td>Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharges, nuclear accidents, and other radiation hazards.</td>
<td>CMM 1.0.1</td>
<td>BCP-01</td>
<td>CMM 1.0.1</td>
<td>BCP-01</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
</tbody>
</table>

### Notes:
- CMM: Common Criteria Maturity Model
- AAS: Auditing and Assurance Services
- ACP: Access Control Policy
- BCP: Business Continuity Plan
- BCP: Business Continuity Planning
- CMM: Common Criteria Maturity Model
- TNM/BNDD: Threat Nutraceutical Bank Deviation Description
- System Type: Application, Systems

---

**HITS Live May 27, 2020**