Enabling continuous risk visibility: The role for OSCAL in revolutionizing third party security

February 2021

Jonathan Dambrot, Principal, KPMG
Adam Brand, Managing Director KPMG
Tom Nash, Manager, KPMG
Agenda

The opportunity  3

Open Security Controls Assessment Language  6

Case study & model demonstration  7

Journey and next steps  12
The changing third party security landscape

Individual assessment

Request for Control Assessment

Client
Industry peer
TP1
TP2

Benefits

— Assessment control questionnaire can be tailored to reflect the organization’s policies and risk appetite.

Challenges

— Significant level of effort and costs associated in the review of third parties.
— High latency as reviews only performed on a 1–3 year cycle.
— Visibility of risk is asymmetric with outsourced risk.
— Lack of standardization.
— Assessment focuses on at the third party enterprise level – not solution that is consumed

Shared assessment model

Request for Control Assessment

Client
Industry peer
TP1
TP2

Benefits

— Efforts and costs shared amongst industry peers.

Challenges

— Doesn’t enable divergent risk appetites.
— Latency remains a problem despite reduced cost burden.
— Visibility of risk remains asymmetric with outsourced risk.
— Assessment continues to focus on at the third party enterprise level – not solution that is consumed
— Limited agreement across industry peers on shared burden, costs, number of third parties etc.
— May still require further client reviews given the organization’s appetite and standards not addressed in shared assessments

Future state

Request for Control Assessment

Client
Industry peer
TP1
TP2

Benefits

— Information gathered can be tailored to the client’s risk appetite.
— Continuous data feed discourages risk acceptance.
— Better visibility of risks into third party environment (operations, system health, security) and management of issues as they arise
— Refocus on monitoring controls specific to the solution provided to the organization

Challenges

— Significant upfront cost (e.g. architectural set up, schema definition)
— Industry standard for this model is still in infancy
— Industry change will require a mindset shift for third parties to conform, allow for integration and freely share their data

Real time control data

TP1
TP2
Industry peer
Client

TP1
TP2
Industry peer
Client

TP1
TP2
Industry peer
Client
The next generation of third party security

Key features

- Facilitates the scalable sharing of control information from third parties to clients
- Agentless in both third party and client environments
- Enables clients to analyze the exposed risk when transacting with any given third-party
- Supports risk visualization, reporting, and issue remediation tracking

1. Aggregator
   - Collects abstracted control data points from relevant solutions (e.g., firewalls, vulnerability management systems)

2. Schema
   - Translates the control data into an agreed schema, ready for receipt and consumption by client

3. Analytics
   - Third-Party control data is aggregated and analyzed (e.g., against the organization’s thresholds, regulatory requirements)

4. Data visualization and workflow
   - Risk and compliance reporting
   - Continues to monitor with real-time incident alerts and dashboards
   - Issue and remediation workflow on third party found issues/risks such as further analysis or policy exceptions
How is 3PS-CAM a game changer?

Client benefits

- Near real-time view on the security risks associated with any given third party
- Ability to track remediation of noncompliant SLAs/SLOs to completion
- Analyze trend data and predict/prevent SLA/SLO noncompliance
- Accelerate agility of the third party security capability

Third party benefits

- Eliminate incremental assessment costs (test once report many)
- Better visibility into your internal systems that manage client environments
- Deeper network integration into client environments
- Quicker and more tailored responses to issues as they arise
### Layers are we focused on

<table>
<thead>
<tr>
<th>Layer</th>
<th>Models/Models (Draft)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assessment Results Layer</td>
<td>Assessment Results Model (Early Access Draft)</td>
</tr>
<tr>
<td></td>
<td>Plan of Action &amp; Milestones (POA&amp;M) Model (Early Access Draft)</td>
</tr>
<tr>
<td></td>
<td>Other Assessment Results Models (Future)</td>
</tr>
<tr>
<td>Assessment Layer</td>
<td>Assessment Plan Model (Early Access Draft)</td>
</tr>
<tr>
<td></td>
<td>Assessment Activity Models (Future)</td>
</tr>
<tr>
<td>Implementation Layer</td>
<td>System Security Plan Model (Draft)</td>
</tr>
<tr>
<td></td>
<td>Component Model (Early Access Draft)</td>
</tr>
<tr>
<td></td>
<td>Other Implementation Models (Future)</td>
</tr>
<tr>
<td>Profile Layer</td>
<td>Profile Model (Draft)</td>
</tr>
<tr>
<td>Catalog Layer</td>
<td>Catalog Model (Draft)</td>
</tr>
</tbody>
</table>

### Attributes benefiting CAM

- Enables the automated assessment of control implementations across multiple components
- Is interoperable and simultaneously supports multiple regulatory frameworks
- Enables monitoring of fourth party risk via the ‘inheritance’ concept
Top 10 Bank and Commercial Lending Platform

KPMG has delivered a proof of concept to demonstrate the effectiveness of this model at a Top 10 Bank (customer) and a Commercial Lending Platform (vendor).

Project outcomes

✓ Collected near real-time technical control data from a third party; continuously.
✓ Standardized control data of a third party through an OSCAL format.
✓ Tested for vendor compliance to contractual SLAs.
✓ Gained insights into vendor’s risk posture through continuous controls monitoring.
✓ Automatically generated issues and response workflows.
✓ Integrated risk view into Client’s existing continuous controls monitoring capability.
Analytics demo 1

![Analytics demo 1](image)
Analytics demo 2
## Illustrative controls for Continuous Assessments and Monitoring

<table>
<thead>
<tr>
<th>Security Domain</th>
<th>Query</th>
<th>NIST 800-53 Reference</th>
<th>Metric Generated</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Loss Prevention</td>
<td>Do systems/applications which host/transmit Customer data have a DLP solution?</td>
<td>SC-7.10</td>
<td>% systems/applications which host/transmit data without DLP solution</td>
<td>Configuration manager DLP system</td>
</tr>
<tr>
<td>Vulnerability Management</td>
<td>Are critical vulnerabilities on internet facing servers and applications patched within 7 days of the patch becoming available?</td>
<td>RA-5.d</td>
<td># patches not installed within 7 days</td>
<td>Vulnerability scan Patch management system</td>
</tr>
<tr>
<td>Encryption</td>
<td>Is all Customer data encrypted in transit and at rest, including laptops, datastores and backups?</td>
<td>SC8.1</td>
<td># systems/applications which host/transmit Customer data and which do not support encryption</td>
<td>Encryption system Configuration manager</td>
</tr>
</tbody>
</table>
How does this model fit into the 3PS ecosystem

**Individual assessments**
- **Focus**: Bespoke policy/process assessments.
- **Illustrative question**: How do you manage SSL server certificate errors?

**Shared Assessments**
- **Focus**: Standardized policy/process assessments
- **Illustrative question**: Do you have a policy covering system configuration?

**Continuous Assessments & Monitoring**
- **Focus**: Technical security controls
- **Illustrative question**: Are internet facing systems/application scanned for misconfigurations?

Holistic, risk based view on third party security
Where are we on the journey?

| **We have completed a proof of concept with a top 10 bank (customer) and commercial lending platform (vendor)** |
|**We are developing pipeline capabilities to enable automated OSCAL reporting** |
|**We anticipate completing solution pilots within the next 3-6 months, post which this model will be ready for scale** |
The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2021 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.