KPMG

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

February 2021

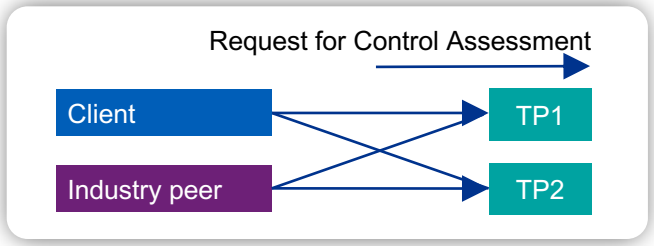
Jonathan Dambrot, Principal, KPMG
Adam Brand, Managing Director KPMG
Tom Nash, Manager, KPMG

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



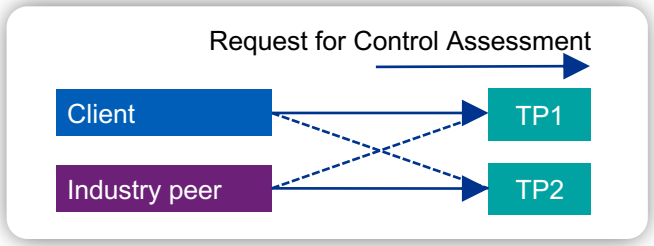
Benefits

— 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



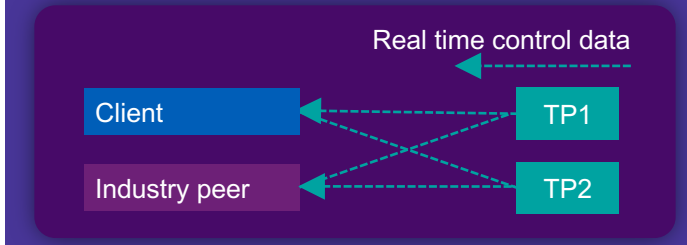
Benefits

— 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



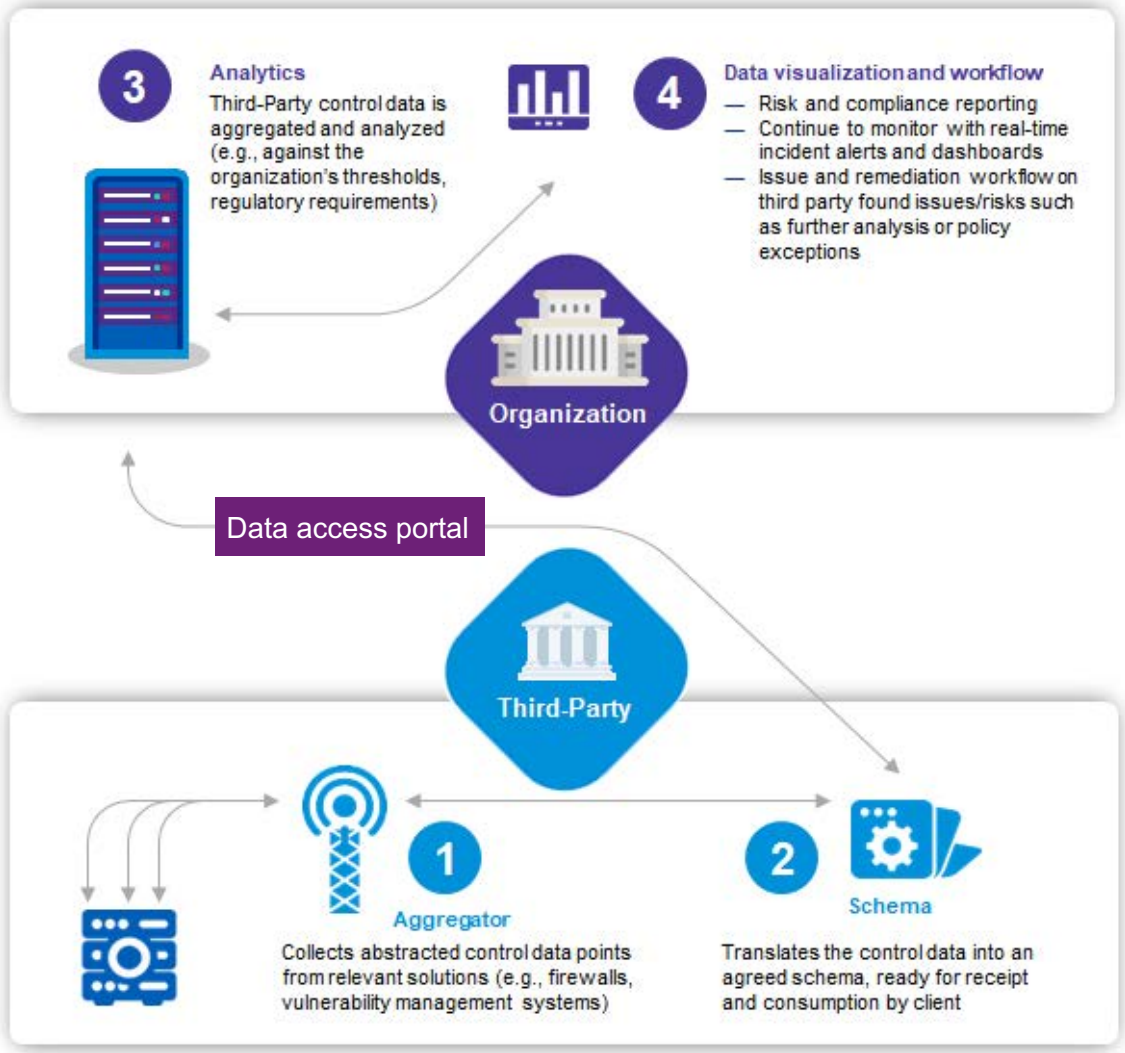
Benefits

— 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

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

How is 3PS-CAM a game changer?

Client benefits

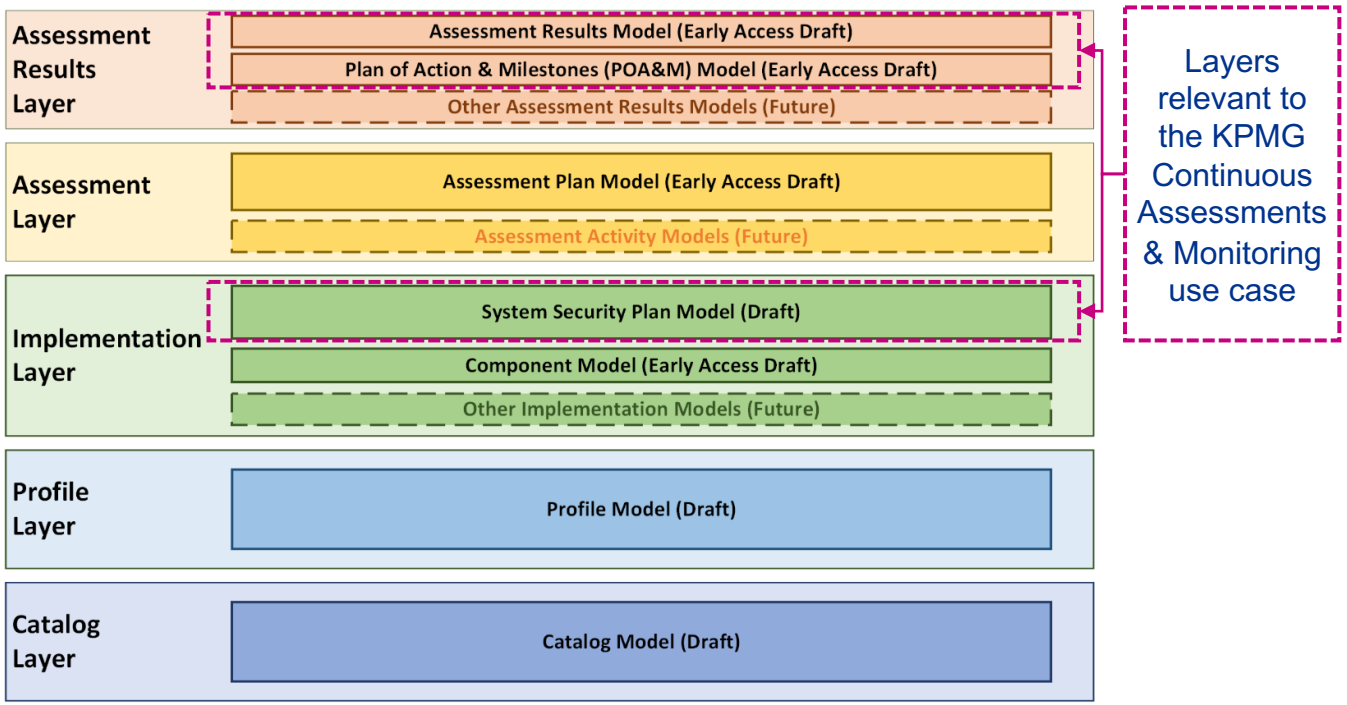
- Near real-time view on the security risks associated with any given third party
- Ability to track remediation of noncompliant SLAs/SLOs to completion
- Analyze trend data and predict/ prevent SLA/SLO noncompliance
- Accelerate agility of the third party security capability

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

OSCAL in Continuous Assessments and Monitoring

Layers are we focused on



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

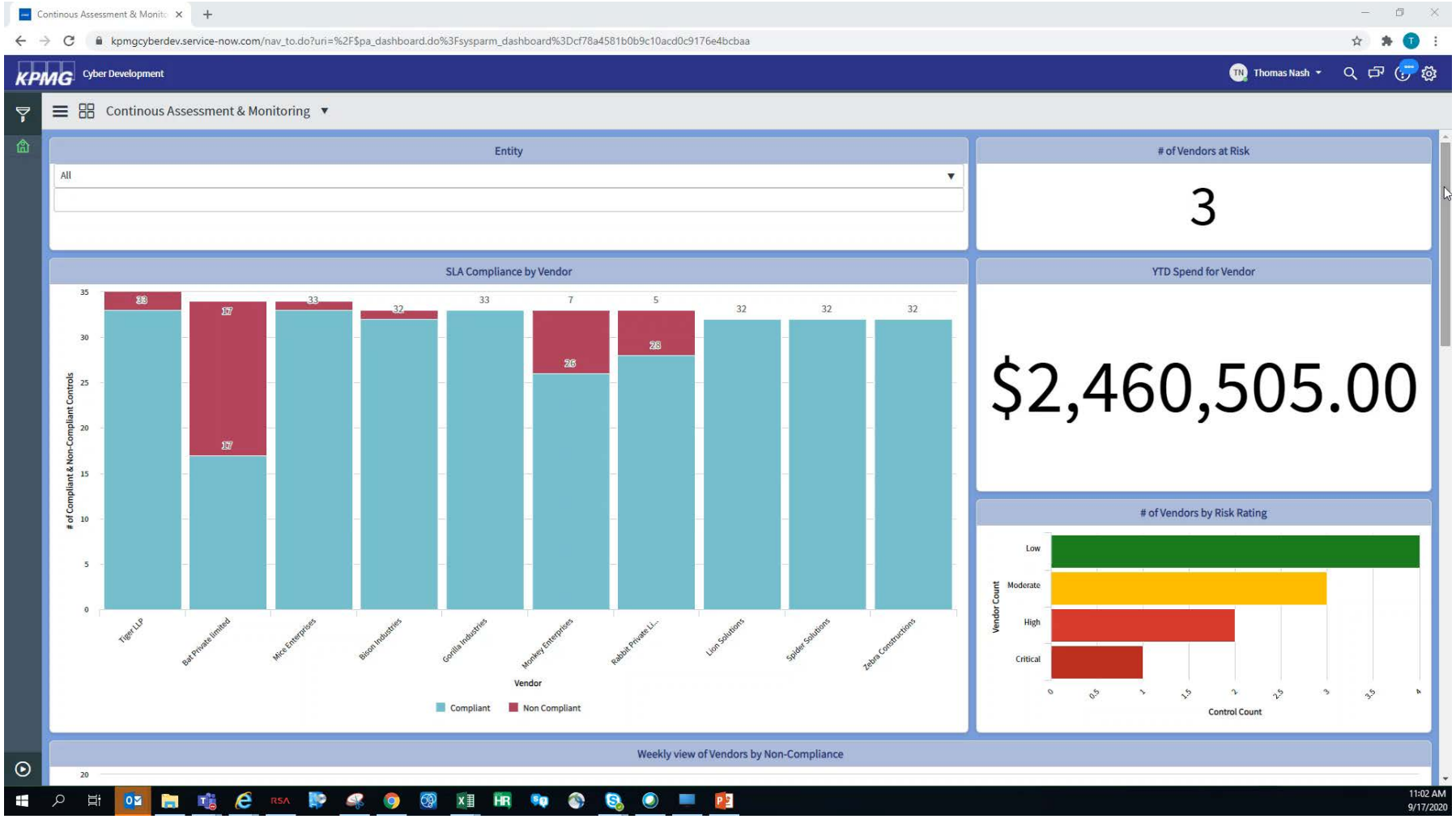
Top 10 Bank and Commercial Lending Platform

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).

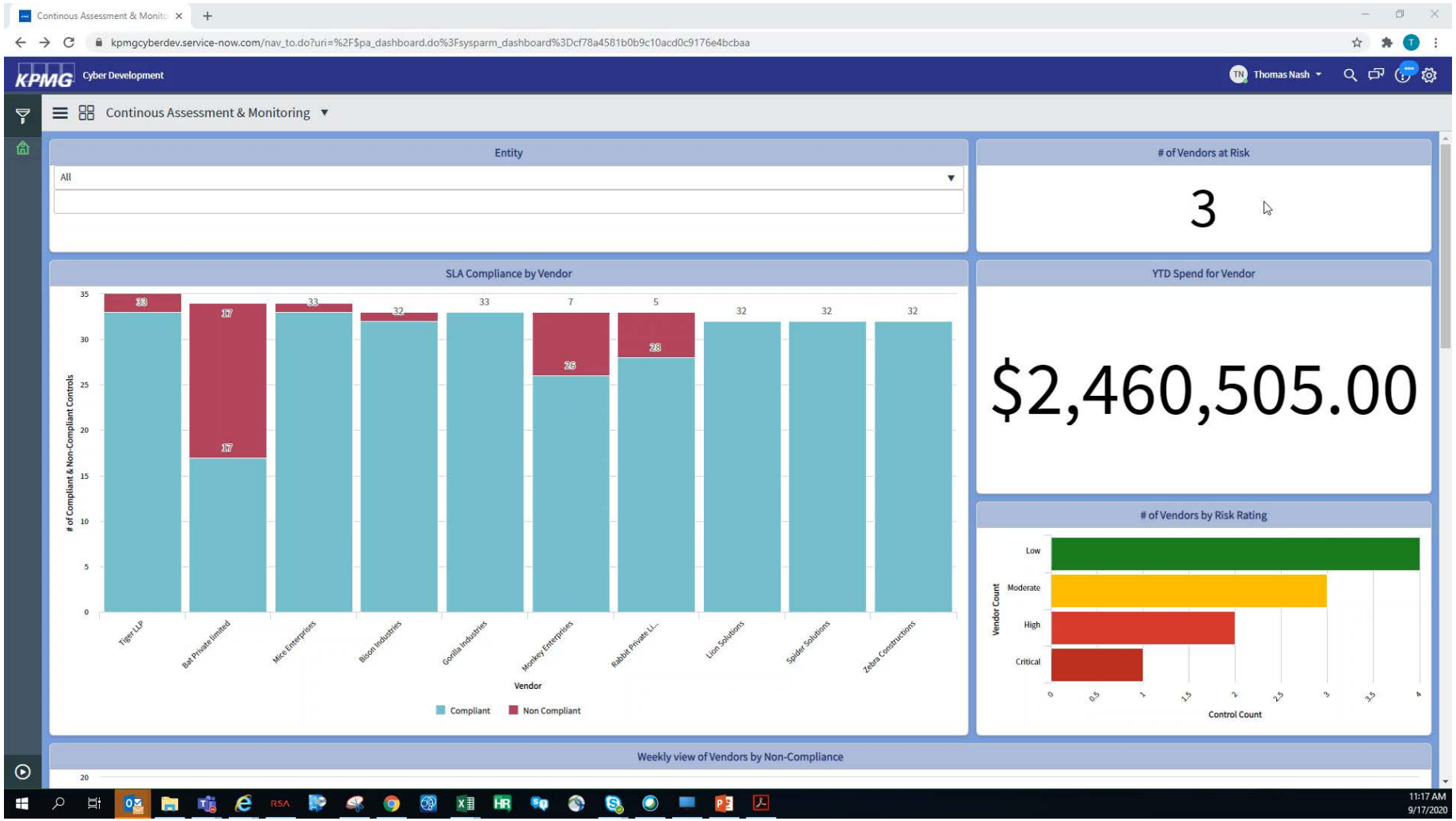
Project outcomes

- ✓ 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 2



Illustrative controls for Continuous Assessments and Monitoring

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

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?

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

Contact us

Jonathan Dambrot
Principal
Cyber Security Services
T: 908-361-6438
E: jdambrot@kpmg.com

Adam Brand
Managing Director
Cyber Security Services
T: 312-282-9878
E: adambrand@kpmg.com

Tom Nash
Manager
Cyber Security Services
T: 347-443-5833
E: thomasnash1@kpmg.com

kpmg.com/socialmedia