# Leading with OSCAL

March 2022

# With you today

**Adam Brand**

KPMG co-lead for OSCAL-enabled capabilities

**Tom Nash**

KPMG co-lead for OSCAL-enabled capabilities

# Contents

- KPMG’s journey with OSCAL
- Commercial sector problem statement
- Commercial sector use cases
- Opportunities to better support commercial use cases
- Our commitments for 2022

# KPMG's journey with OSCAL

**We have developed multiple use cases that are powered by OSCAL.**

These all leverage the key benefits of OSCAL:

- Data centric
- Integrated
- Extensible
- Automated

**Third-party security**

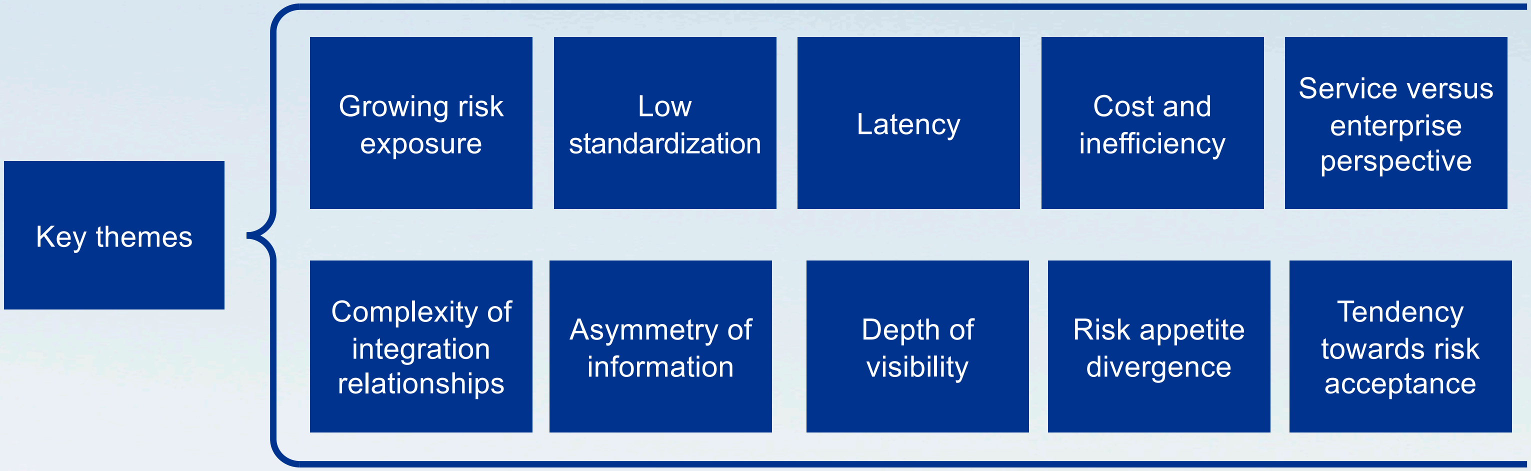
**Fourth-party security**

**Cyber insurance**

**Private equity portfolio monitoring**

**Compliance reporting**

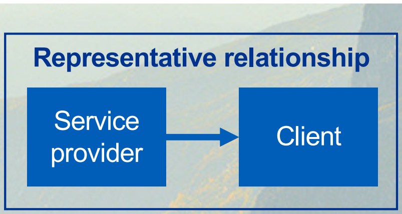
# Commercial sector problem statement



Key themes

- Growing risk exposure
- Low standardization
- Latency
- Cost and inefficiency
- Service versus enterprise perspective
- Complexity of integration relationships
- Asymmetry of information
- Depth of visibility
- Risk appetite divergence
- Tendency towards risk acceptance

# Third Party Security



## Problem statement

- Proliferation of vendors
- Reassessment trigger visibility
- Culture of risk acceptance
- Low security ROI

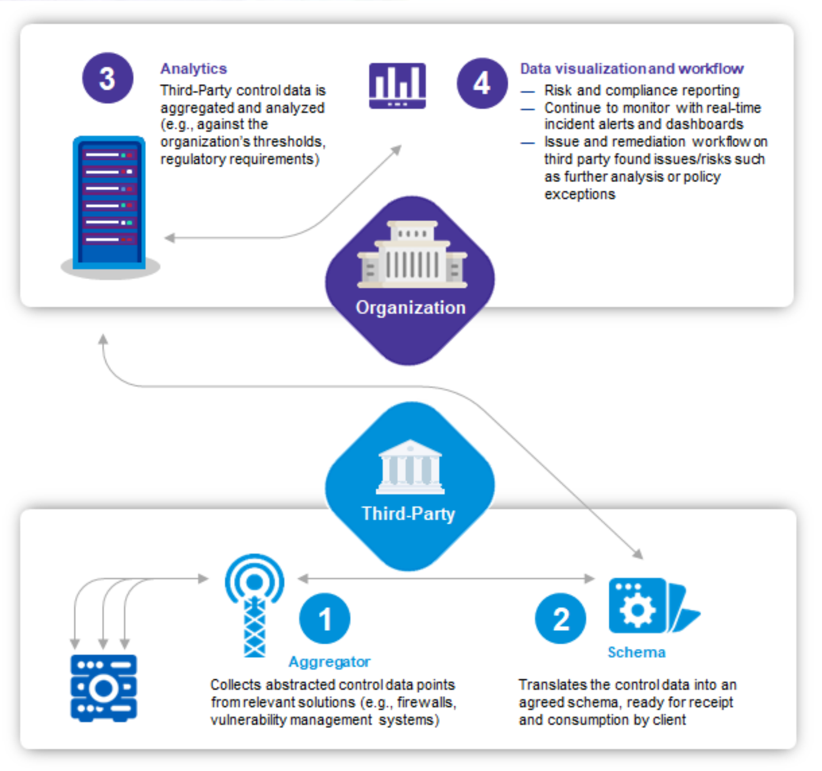
## Illustrative use case

- Organization performs annual assessments on high risk vendors
- No visibility into security posture post events
- Requirement for more real-time data

## KPMG experience

- Developed model
- Delivered POC
- Actively discussions ongoing

# Third Party Security: Our OSCAL journey started



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
— Continue 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

1 Aggregator

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

2 Schema

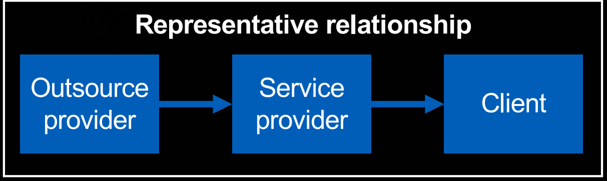
Translates the control data into an agreed schema, ready for receipt and consumption by client

## Key features

- Facilitates scalable sharing of control information
- Agentless
- Analyze cyber risk
- Risk reporting and issue remediation

KPMG

# Fourth-party security



Representative relationship

**Problem statement**

- Service vendors often outsource
- Difficult to inventory fourth parties
- No contractual relationship with fourth parties

**Illustrative use case**

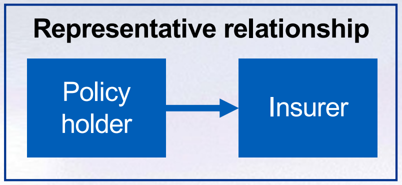
- Better manage cyber risk
- Service providers report OSCAL
- Service provider can “inherit” ARs

**KPMG experience**

- Involvement in defining “leading practice” for 4PS
- Architected KPMG CAM to support 4PS use cases

KPMG

# Cyber insurance


Representative relationship

Policy holder

Insurer

## Problem statement

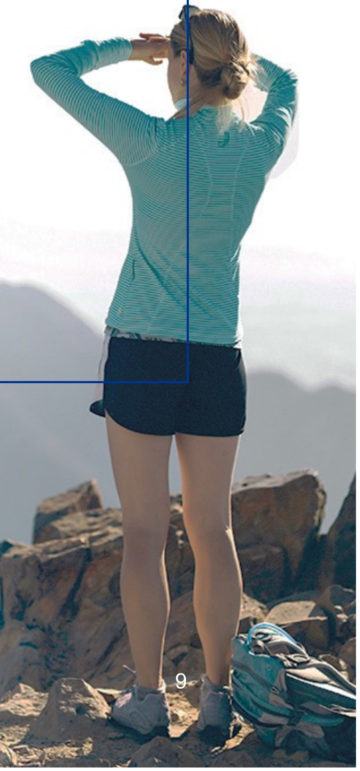
- Pricing of cyber insurance policies
- Demand / supply mismatch
- Cyber insurers are making losses

## Illustrative use case

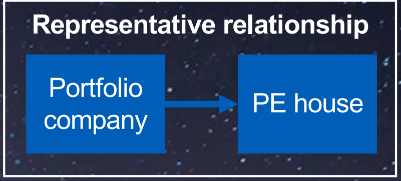
- Aggregate cyber risk across portfolio
- Correlation between weak controls and losses
- Updates contracts with additional requirements a

## KPMG experience

- Facilitated industry event



# Private equity portfolio monitoring


Representative relationship

## Problem statement

- Breaches impact valuations
- PortCos managed separately

## Illustrative use case

- PE house receives threat intel
- Threat intel communicated to PortCos

## KPMG experience

- Working with multiple PE houses

# Opportunities to better support commercial use cases

1. Catalog models for additional reference frameworks
2. Native support for integrity and provenance validation
3. Tooling to support human read- and writability
4. Native support for OSCAL in other security tools
5. Enhance GRC enablement
6. Standardized approach for a mechanism to obtain compliance status
7. Better support for schema customization based on use case

# Our commitments for 2022

1

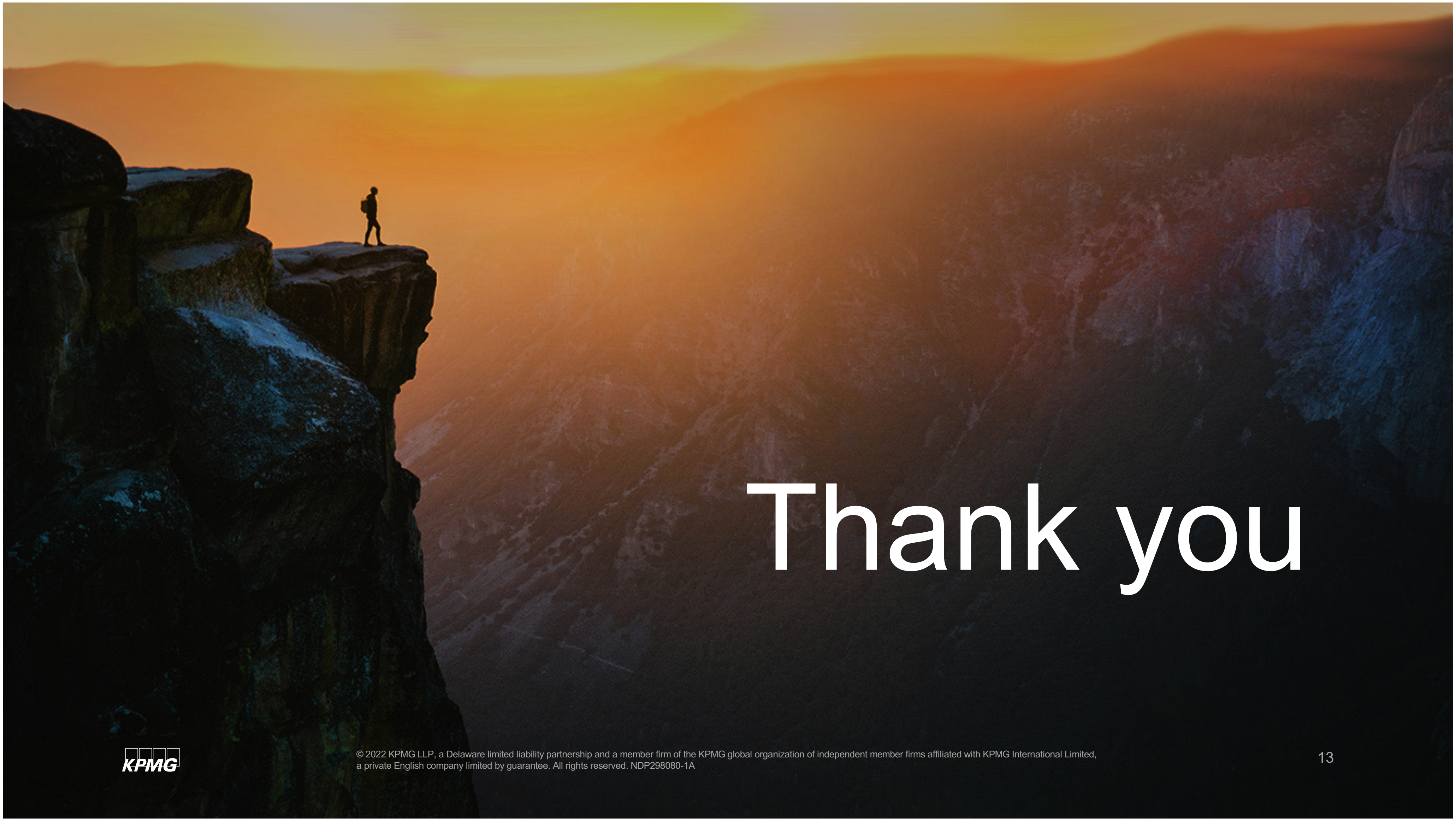
Active client outreach—expand awareness and broaden the conversation

2

Investment in integrating OSCAL into the services we deliver

3

Continue to lead on commercial sector use case development



# Thank you

KPMG

## Contact us

**Adam Brand**
Managing Director
312 282 9878
adambrand@kpmg.com

**Tom Nash**
Director
347 443 5833
thomasnash1@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

**kpmg.com/socialmedia**

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.