

The logo for FORVIS, featuring the word "FORVIS" in a bold, red, sans-serif font. The letters are slightly italicized, with the 'V' and 'I' having a slanted appearance. The logo is positioned on the left side of the slide, against a white background. To the right of the logo, there is a large, dark gray graphic consisting of several overlapping, parallel diagonal lines that create a sense of depth and movement, extending from the top right towards the bottom left.

# FORVIS

## Third-Party Risk Management & Governance

December 2022

# TPRM Purpose & Strategy Objectives

Third-Party Risk is the risk associated with outsourcing an internal business function to an outside party and is a growing regulatory focus with respect to operational resiliency and sustainability. It is an extension of Enterprise Risk Management and spans a multitude of ERM risk categories which can be operational, strategic or financial in nature. As such, it should have its own set of comprehensive policies, procedures, governance structures, and risk taxonomies.



## Third-party Risk Program Objectives

### Risk Appetite Alignment



- Clearly articulates Third-Party performance standards and expectations, which enables execution of long-term procurement strategy
- Manages key vendor risks to ensure adherence to the enterprise's Risk Appetite

### Strong Risk Culture



- Generates awareness around the growing prevalence and complexity of Third-Party relationships in order to promote an informed, organization-wide risk culture
- Creates a "tone-from-the-top" environment through consistent messaging and commitment from leadership

### Greater Accountability



- Bolsters accountability across Third-Party governance groups, committees, and escalation/reporting structures to effectively manage outsourced functions, regardless of their complexity
- Allows for more timely detection and handling of Third-Party performance and risk issues

### Internal & Regulatory Compliance



- Strengthens evidence and inventory management for compliance with key Third-Party regulations (GDPR, HIPAA, ESMA, FDIC, OCC, etc.)
- Facilitates internal recordkeeping, policy maintenance, and training which are key for program maturity



# Polling Question 1

Our Third Party risk management function is:

- a. Very limited or non-existent
- b. Being developed and provides some coverage of known exposures
- c. Fully functioning and covers most known exposures

# TPRM Lifecycle Overview

Displayed is the TPRM Lifecycle and an overview of activities completed across the 3 Lines of Defense (LoD). Such activities are enabled through considering the following areas:

- **Risk Profiling:**  
How do we determine the probability of loss and organizational impact from working with a Third-Party?
- **Inventory:**  
How should we store pertinent Third-Party intake and assessment information for easy retrieval?
- **Reporting:**  
How do we communicate TPRM information to internal and external stakeholders?
- **Technology:**  
Which tools and platforms can enable accurate and timely assessment and monitoring?
- **Operating Model:**  
How should internal stakeholders interact and communicate to achieve this desired state?

## I. Planning

- Identify business need for a Third-Party
- Initiate centralized sourcing process and RFPs
- Determine Third-Party's Criticality/Impact to the business
- Document exit strategies

## II. Due Diligence

- Risk-based assessments across Risk Domain Areas (RDAs), utilizing internal/external tools and SME input
- Issues management, escalation, and remediation
- Regulatory considerations

## III. Contracting

- Modification of protective language to consider due diligence findings
- Negotiation and signing
- Central contract maintenance, in compliance with internal and regulatory retention requirements

## V. Offboarding

- Implementation of exit strategy (transition in-house or to alternative provider)
- Termination checklist (termination of access, certification of destruction or retrieval)



## IV. Ongoing Monitoring

- Periodic re-assessment of Third-Party's risk level
- Revalidation of scope assumptions (i.e., has the nature of our relationship changed? Are they handling more sensitive data than they were before?)
- Recalculation of risk profile
- Issues management
- Independent evaluations for TPRM program adequacy

# Planning


Planning involves identifying the need for outsourcing and gathering intake data to assess the criticality (i.e., impact) of the Third-Party to your organization. The Third-Party should also be assigned an Exit Strategy to outline how services will be transitioned in-house or to an alternate provider, in the event there are changes to internal strategy or the Third-Party is no longer able to execute the terms of its agreement. A disjointed sourcing process which lacks ownership can result in time unnecessarily spent filling data gaps, and lack of contingencies can lead to significant service disruption during offboarding.

## Key Steps

- Conduct an inventory of your current procurement workflows and vendor intake forms to diagnose bottlenecks and data gaps in Third-Party onboarding.
- Implement a preliminary intake questionnaire which assesses the Third-Party's criticality based on key relationship attributes such as its level of network access, impact on business continuity, and impact on regulatory requirements.
- Develop risk criteria relevant to the organization and rank potential Third-Parties ( IT Data Security/ Non-IT Exposures)
- Design and assign ownership to a centralized repository to house Inventory data such as Third-Party location, type of data access, risk level, signed contract and more

# Third Party Inventory

A mature TPRM Program should also have a dedicated, organized, and easily-retrievable inventory which maps to your procurement workflows. The inventory captures all Third-Parties and related Lifecycle documentation such as the internal Relationship Owner, criticality, assessment results, contracts, SLAs, and known issues and their remediation status. Lack of visibility into the distribution and profiles of your Third-Parties can result in underassessing higher-risk vendors or overlooking special circumstances which require SME or Compliance review.

Supplier Name	Supplier ID	Sourcing Request ID	Dates Effective	Expiration Date	Project Name	Signing/Requesting Entity	Risk Management Profile
Dixon Hughes Goodman LLP	001	PR123456	01/01/2022-6/31/2022	6/31/2022	TPRM Development	Name of the department or subsidiary requesting outsourced function	

Relationship Owner

John Smith


Criticality Tier

2


Risk Rating

High

Issues

1. 4/05/22  
Response: Remediate/Accept  
Remediation Status: Open/Closed  
Remediation Plan:   
Due Date: 5/05/22

Contract





ILLUSTRATIVE

# Polling Question 2

We have a complete inventory of our critical vendors:

- a. Yes
- b. No

# Due Diligence

The scope of risk-based due diligence conducted on a Third-Party should be commensurate with its criticality to your organization. Subjecting all Third-Parties to the same type of reviews, irrespective of the type or scope of their function, can hinder effective detection of trends and issues. Depending on their size and industry, Third-Parties may also provide insufficient or no answer to general information requests, making it difficult to assess their riskiness. Developing specific, targeted assessments for your Third-Party will improve supplier communication and transparency to ensure that their governance standards and risk profile align with your goals.

The **Third-Party** should be assessed across Risk Domains.



- Information Security
- Information Technology
- Reputation
- Strategic Fit
- Corporate Governance
- Business Continuity
- Regulatory & Compliance
- Financial Health
- Country
- Fourth-Party



# Due Diligence: TPRM Tool Enablement

Below are examples of industry-leading TPRM tools that can aid in data collection and workflow automation for your Third-Party Lifecycle.

	Venminder	BitSight	Aravo	Prevalent	OneTrust
<b>Planning</b>	<ul style="list-style-type: none"> <li>Vet completeness and accuracy of vendor intake data</li> <li>Determination of critical and high-risk vendors</li> </ul>	<ul style="list-style-type: none"> <li>Specializes in Information Security and Cyber Risk</li> <li>More data-focused, less emphasis on holistic lifecycle integration</li> </ul>	<ul style="list-style-type: none"> <li>Screen for pre-qualified vendors and vendor overlap</li> <li>Capture criticality and inherent risk</li> <li>Self-service vendor portal for uploading policies, COIs, etc.</li> </ul>	<ul style="list-style-type: none"> <li>Different levels of packages available</li> <li>Tier vendors based on criticality of the service</li> <li>Quantify inherent risk to clarify where to focus vendor assessments</li> </ul>	<ul style="list-style-type: none"> <li>Create central vendor inventory and build individual vendor profiles</li> <li>Automated inherent risk insights to prioritize critical vendors</li> </ul>
<b>Due Diligence/ Monitoring</b>	<ul style="list-style-type: none"> <li>Determine what and how much due diligence needs to be done</li> <li>Control assessments performed by SMEs to evaluate and assign risk level</li> <li>Customize risk level and scoring terminology</li> <li>Continuous monitoring</li> </ul>	<ul style="list-style-type: none"> <li>Compare inherent risk to Third-Party's security rating</li> <li>Validate security controls across new and existing vendors</li> <li>Data integrates with GRC, ServiceNow, Venminder, ProcessNow, ThirdPartyTrust, etc.</li> <li>Continuous monitoring to enable evidence-based remediations</li> </ul>	<ul style="list-style-type: none"> <li>Utilizes dynamic self-assessment questionnaires and Aravo's automated risk scoring algorithm</li> <li>Automatic workflows trigger</li> <li>Vendor performance and issues management, including remediations</li> <li>Integrates with content from Refinitiv, Dow Jones, Security Scorecard, BitSight, etc.</li> </ul>	<ul style="list-style-type: none"> <li>Risk scoring, assessment, and benchmarking of vendors against industry frameworks</li> <li>Recommends remediations to mitigate residual risk</li> <li>Built-in report templates to identify and communicate risk exceptions</li> <li>Map assessment results to any regulation or framework</li> </ul>	<ul style="list-style-type: none"> <li>Dozens of assessment templates and questionnaire builder</li> <li>Editable questions, rules logic, and risk scoring</li> <li>Track compliance details and critical metrics</li> <li>Monitor both risk and performance using automation engine to remediate issues</li> </ul>
<b>Contract Management</b>	<ul style="list-style-type: none"> <li>Contract compliance assessment</li> </ul>		<ul style="list-style-type: none"> <li>Create centralized contract repository</li> </ul>	<ul style="list-style-type: none"> <li>Contract assessment</li> <li>Workspace for contract task management, discussions, and document storage of NDAs, SLAs, SOWs, and contracts</li> </ul>	<ul style="list-style-type: none"> <li>Extract contract terms relevant to internal stakeholders and set triggers for reassessments</li> </ul>
<b>Offboarding</b>	<ul style="list-style-type: none"> <li>Workspace to manage terminations via dashboard of tasks, forms, and adherence to exit strategy</li> </ul>		<ul style="list-style-type: none"> <li>Manage offboarding workflows via termination notifications, capture data privacy and destruction attestations, disable physical/logical access, finalize payments</li> </ul>	<ul style="list-style-type: none"> <li>Customized surveys to report on systems access, data destruction, regulatory compliance, and final payment</li> </ul>	

# Polling Question 3

We obtain assurance reports (SOC1, SOC2, etc.) on our critical vendors:

- a. Yes
- b. No

# Contracting and Monitoring



## Contracting

Failing to consider the unique circumstances of a vendor relationship in your contract can lead to risk and performance issues downstream. Before conducting negotiations and executing the written agreement, your team should modify any standard legal contract templates to address unique circumstances, issues, and regulatory obligations applicable to the Third-Party. A contracting process which prioritizes stakeholder feedback and sign-off will ensure that contracts hold Third-Parties to a sufficient level of accountability and are not binding until the 1st Line of Defense is comfortable with the risks assumed.



## Monitoring

An effective TPRM Program ascertains the appropriate scope and frequency of Third-Party monitoring and will enable timely detection of performance and risk-related issues.

### Key Steps

- Determine monitoring areas and frequency that are most appropriate for low and high-impact vendors
- Create a monitoring schedule which details how frequently Third-Party risk profiles should be re-evaluated to support trend detection and risk appetite alignment
- Obtain and analyze assurance reports (SOC1, SOC2, etc.)
- Identify and inventory Third-Party subservice providers ( Fourth-Party risk)
- Create Issues Management processes which assign accountability to the execution of remediation plans

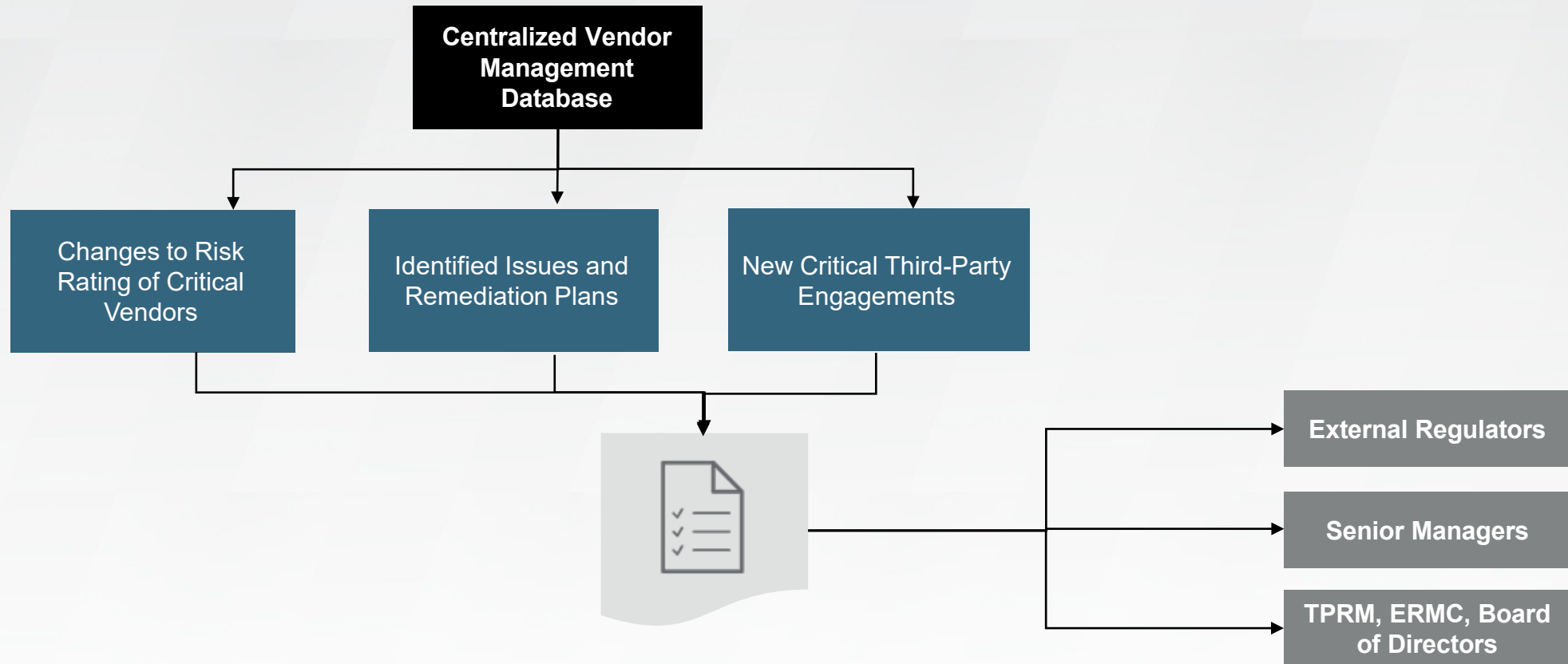
# Offboarding

When internal strategy changes or the Third-Party is no longer meeting its service-level agreements, exit strategies should be executed to transfer Third-Party resources and activities in-house or to an alternate provider. Following a termination checklist will help to avoid prolonged service disruption and confusion over which departments are involved in offboarding.

A. Implementation of Exit Strategy	Termination Requirements	Guidance and Follow-up Tasks for Relationship Owner	Deadline	Completion Status	Completion Date	Required Termination Plan Documentation
B. Validation of Contractual Rights and Obligations						
C. Notification to Impacted Stakeholders/Risk Domain SMEs						
D. Return/Removal/Disposal of Data and Assets						
E. Knowledge Transfer						
F. Termination of Logical and Physical Access						
G. Documentation of Termination Plan						

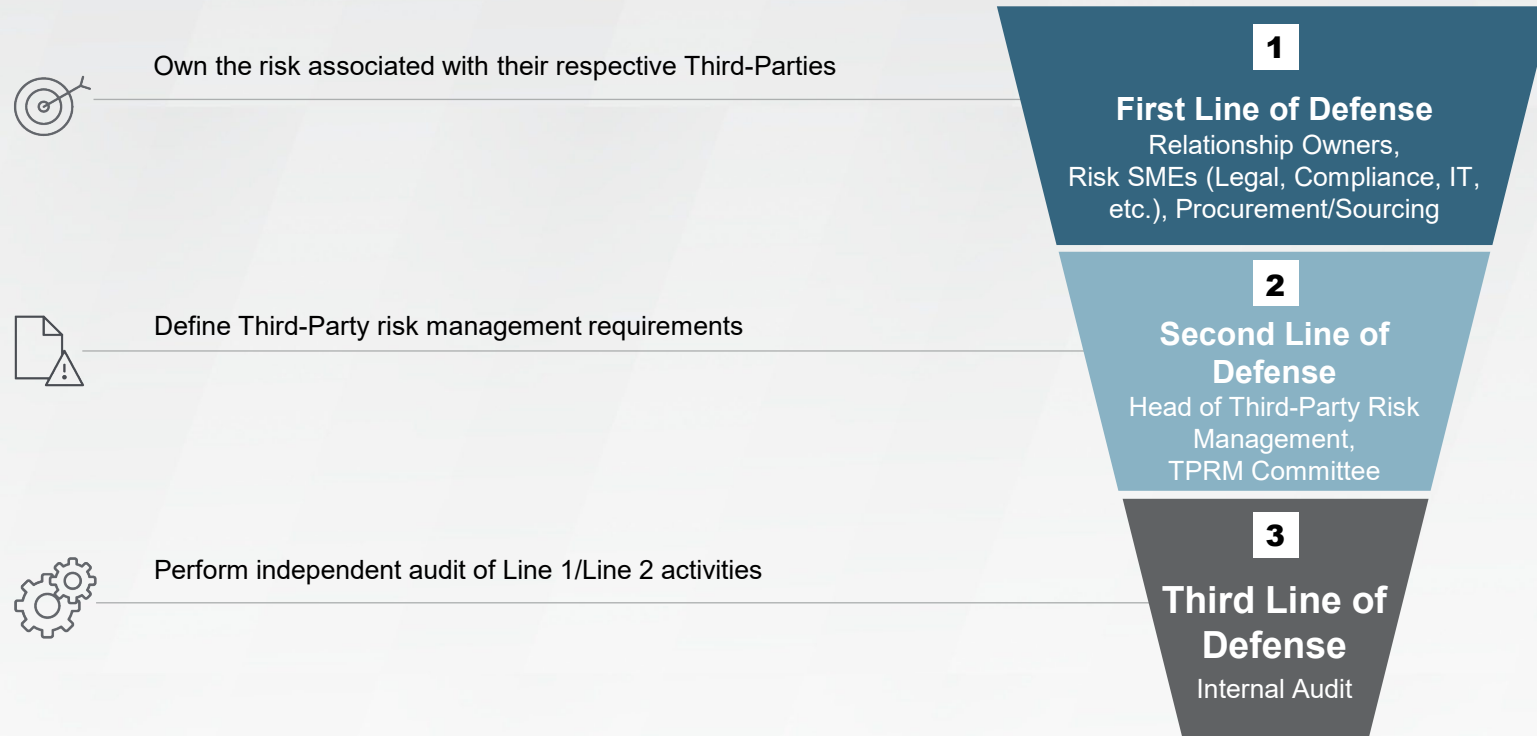
# Reporting

Significant changes to Critical/Tier 1 vendors, due diligence/ongoing monitoring findings, and/or Third-Party risk strategy should be reported to senior management at least quarterly and to regulators as required. TPRM reports should use clearly-defined KRIs and should be developed and challenged by all three Lines of Defense in order to draw intelligent insights on the aggregate Third-Party risk profile.



# Roles & Lines of Defense

A robust TPRM program utilizes multiple organizational layers to design, implement and enforce risk management activities.



## Key Responsibilities For Relationship Owners

- Act as a front-line interface for Third-Parties and own risks associated with engaging Third-Parties for products and/or services
- Monitor and manage Third-Party performance on an ongoing basis
- Monitor risks/issues and drive action plans with Third-Parties
- Provide Third-Party risk metrics, report to executives, and escalate issues/risks

# Polling Question 4

We have a second-line of defense function or committee that supports oversight on third-party risks?

- a. Yes
- b. No

# TPRM Maturity Model

	Initial	Repeatable	Defined	Managed	Optimizing
Governance	There are no documented TPRM policies or procedures.	TPRM policies and procedures have been conceptualized and/or are in development, but there may be confusion over roles and responsibilities.	TPRM policies and procedures have been defined at the departmental level, but execution is lacking.	TPRM policies and procedures are well defined and operationalized but continue to be carried out in silos.	TPRM policies, procedures, roles, and responsibilities are well-defined across the organization to allow for cross-functional governance.
Planning	A Third-Party inventory does not exist and/or we are unsure how many Third-Parties we use.	We have an inventory from which information can be retrieved, but it only tracks critical Third-Parties and/or some Third-Parties are missing.	We document all Third-Party engagements in an inventory but are unclear on Procurement processes and/or what data is collected.	All Third-Parties are inventoried, including their materiality and risk profiles, but ownership of data is still unclear and/or there are significant data gaps.	We have a well-documented, organized inventory for all Third-Parties that captures their materiality and risk profiles, know who owns the data, and how to retrieve it.
Due Diligence/ Monitoring	Third-Parties are assessed across a few risk areas but domains are not comprehensive. Assessments are commonly done using spreadsheets, emails, and/or holistic evaluations. Risks are only assessed during onboarding with no process for reevaluating risk level.	Some technology is used in Third-Party assessment, but they are mostly legacy governance, risk, and compliance tools. Risks are only reassessed upon contract renewal.	We utilize up-to-date technology for due diligence assessments, but it is spread out across departments with little communication or feedback across SMEs. Risks are reassessed periodically according to the Third-Party's criticality, but we lack issues management processes to address these findings.	We utilize integrated, specialty TPRM technology to assess Third-Parties and we reassess risk level periodically according to Third-Party's criticality. We are still developing issues management processes but have not yet assigned ownership to tracking remediations.	Third-Parties are assessed comprehensively across risk domains and assessments are tailored to the nature of the engagement. We use TPRM specialty tools which align to our organization's risk framework. We have issues management processes with well-defined roles and responsibilities and remediation plans. Risks are reassessed immediately as changes in risk profile trigger review.
Reporting & Analytics	Little to no reporting is done on Third-Party performance and risk metrics.	We have defined Third-Party metrics and know how to create reports, but they may not provide meaningful insights or allow for strategic decision making.	Reporting is conducted haphazardly or as needed and may not involve the correct stakeholders.	Reports are compiled at regular intervals but are carried out at the department level, making it difficult to gain a holistic view of Third-Party risk trends.	Third-Party performance and risk metrics are reported at frequencies commensurate to your organization's risk appetite and involve input from all SMEs. Metrics allow you to see aggregate and engagement-level risk or performance trends.



# Questions

**forvis.com**

The information set forth in this presentation contains the analysis and conclusions of the author(s) based upon his/her/their research and analysis of industry information and legal authorities. Such analysis and conclusions should not be deemed opinions or conclusions by FORVIS or the author(s) as to any individual situation as situations are fact specific. The reader should perform its own analysis and form its own conclusions regarding any specific situation. Further, the author(s) conclusions may be revised without notice with or without changes in industry information and legal authorities. FORVIS has been registered in the U.S. Patent and Trademark Office, which registration is pending.

**FORVIS**

Assurance / Tax / Advisory