hfma
ma-ri chapter

NEW ENGLAND HEALTHCARE INTERNAL AUDITORS INC.

HFMA/NEHIA

2024 Compliance & Internal Audit Conference

Wednesday, December 4 - Friday, December 6, 2024
Mystic Marriott Hotel, Groton, CT

NEHIA/HFMA

2024 Compliance & Internal Audit Conference

Wednesday, December 4 - Friday, December 6, 2024

Mystic Marriott Hotel, Groton, CT

Agenda

1. Understanding the TPRM landscape, including regulatory requirements
2. Review of an enterprise TPRM framework
3. Defining stakeholder roles, governance, and integrations with other functions
4. Walkthrough of a typical TPRM technology solution architecture
5. Actioning these key topics through roadmap development

Why are we focusing on TPRM?

A broad set of third-party risk drivers…

External

- Increasing dependency on third and fourth parties
- Evolving regulatory landscape
- Consumer concerns for sustainability and corporate citizenship ("ESG")
- Digital and social media
- Unforeseen disruptions (e.g., pandemic, earthquake)
- Cost and profitability pressures
- Globalization and trade

Internal

- Evolving operating and business models
- New and complex channels
- Impact of data breaches/ ransomware
- Supply chain resiliency and reputational risks
- Increasing compliance costs (across Cyber, Procurement, Legal, Compliance, etc.)
- Audit findings

…are driving increased focus and investment

1. Board involvement in TPRM has increased to 32% of surveyed organizations (up from 24% in 2018)
2. Various states and jurisdictions (e.g., SEC) have called for increased transparency into the security and privacy posture of companies
3. 38% of organizations have experienced a data breach caused by a third party over the past 2 years; 52% have experienced an outage
4. 84% of organizations said that failures stemming from not identifying third-party risks resulted in key operational disruptions

While there are risks, organizations are realizing the benefits of a TPRM program…

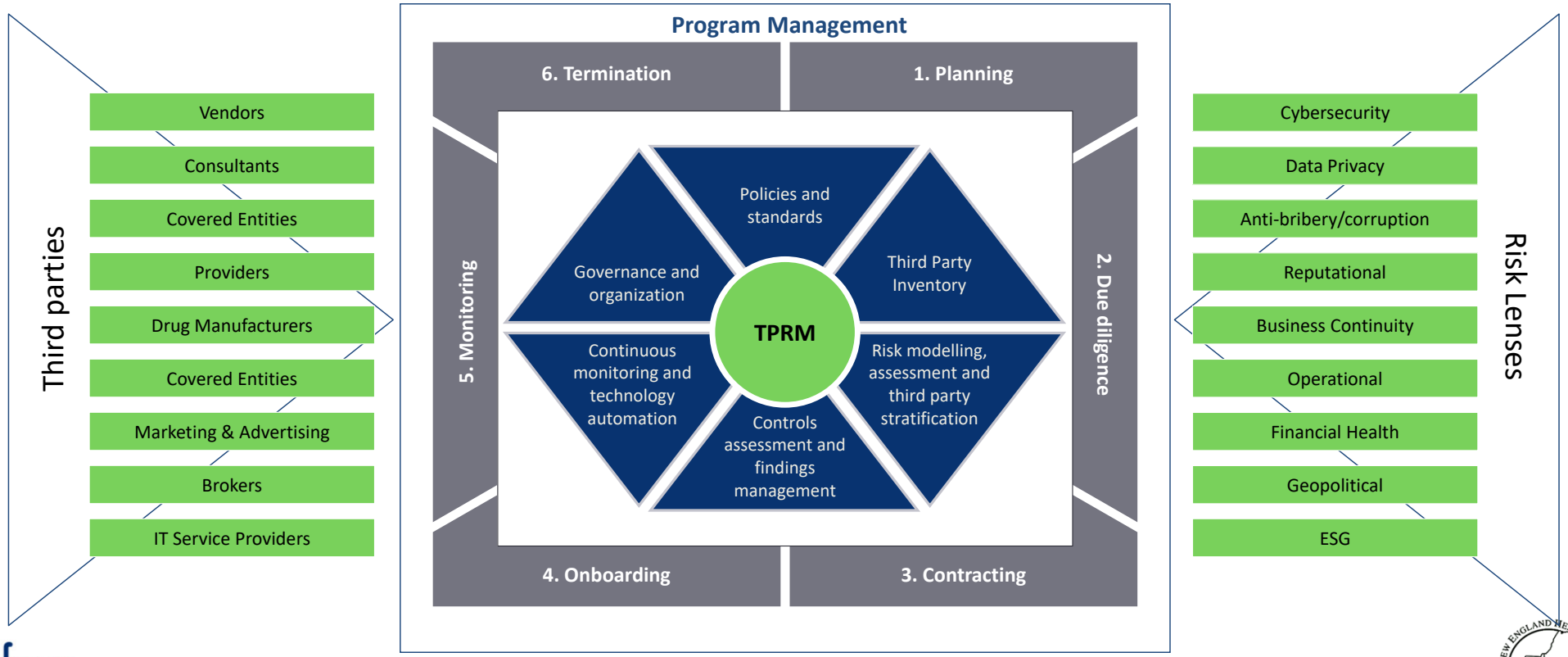
Increased buying power	Managed risk-taking	Improved resiliency posture
Greater visibility to third parties	Regulatory compliance	Increased business agility

hfma ma-ri chapter

New England Healthcare Internal Auditors Inc.

Embedding end-to-end visibility, simulation & risk monitoring across supply chains

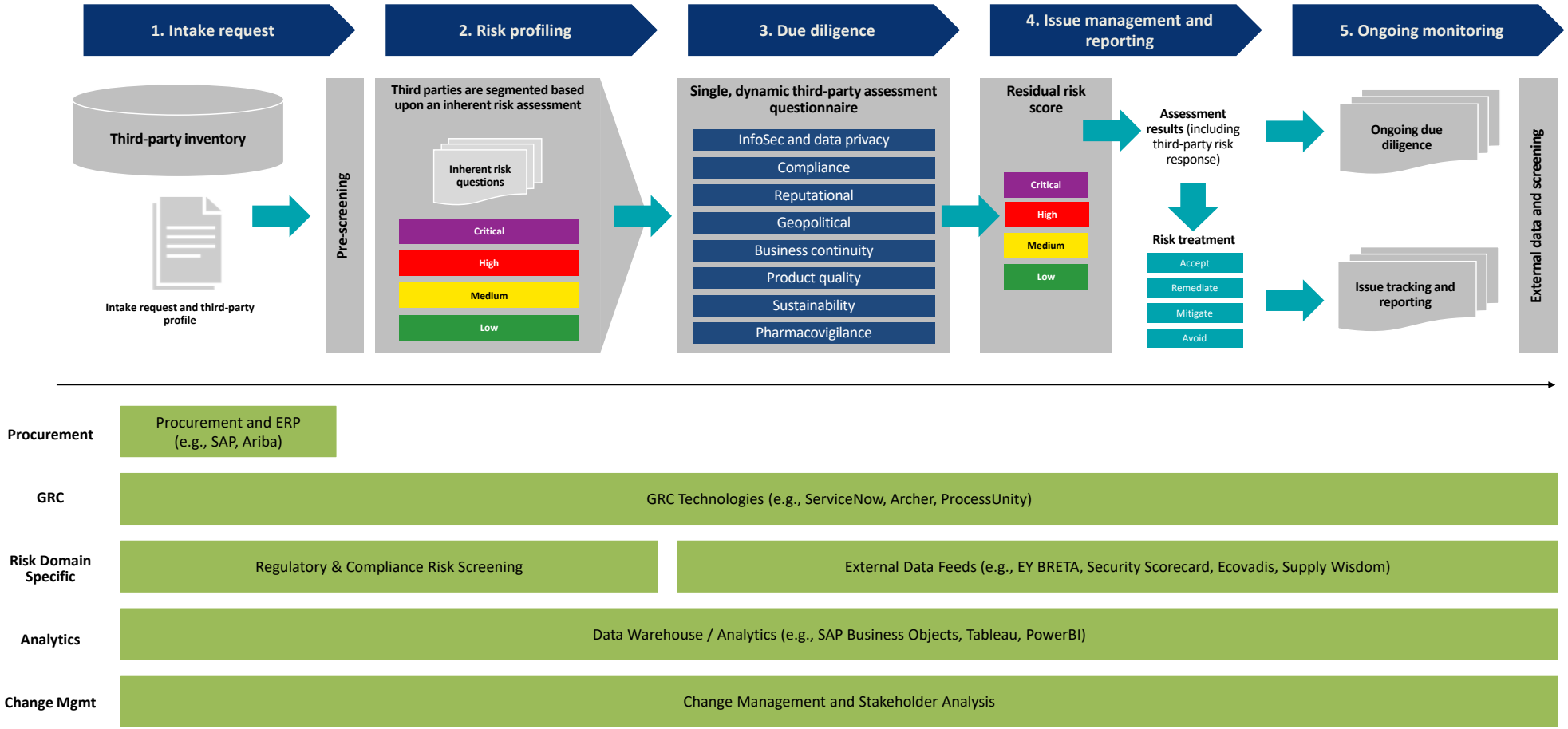
TPRM provides a function for management to identify, evaluate, monitor and manage the risks associated with third parties (e.g., vendors/suppliers, intercompany relationships and fourth parties).



hfma ma-ri chapter

New England Healthcare Internal Auditors Inc.

Leading organizations develop a streamlined third-party risk management process that applies a risk-based approach to managing risk



Governance and oversight: Sample governance model including three lines of defense

The “three lines of defense model” or lines of defense (LOD) model is widely adopted and considered industry practice by organizations operating in more highly regulated sectors or that are global and complex in nature.

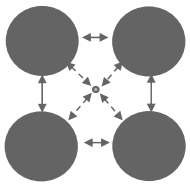
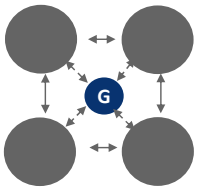
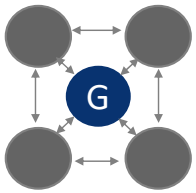
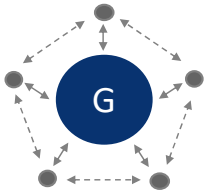
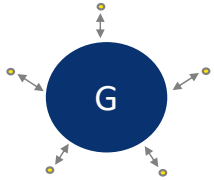
The following is an example of a lines of defense model for TPRM:

	Board of directors		
	First line: business	**Second line: risk management**	**Third line: audit**
Roles and responsibilities	► Owns the third-party relationship (from onboarding through offboarding) ► Identifies, assesses, monitors, and manages the risks associated with the third-party (business is engaging the third-party and owns the risk) ► Implements the capabilities and processes required to manage third-party risks, including the ongoing monitoring and reporting	► Provides expectations and guidelines for managing third-party risk ► Develops enterprise-wide guidance and policies, including defining roles and responsibilities ► Provides guidance to the business around implementing a TPRM framework ► Assists with defining acceptable levels of risk-taking and identifying known and emerging risks ► Monitors implementation of TPRM capabilities and processes by the business	► Independently assesses TPRM capabilities and processes, including adherence to the organization’s policies and framework ► Provides assurance that TPRM processes are designed and operating effectively ► Identifies improvement opportunities
Key challenges	► Understanding the potential risk exposure to adequately assess and manage the third-party ► Determining the potential impact to the organization (e.g., processes) should a risk occur ► Integrating third-party risk activities within third-party management activities	► Maintaining independence while providing meaningful insight and support to the business ► Understanding overall third-party risk exposure to the organization ► Minimizing duplicate efforts between first and second line as well as with first line functions	► Minimizing duplicate efforts ► Applying a risk-based approach versus a coverage-based approach ► Understanding and communicating potential risk exposure

Understanding and considering the operating model to support the TPRM program across the organization

Organizations most often adopt more centralized governance and operating models to simplify and standardize third party risk activities, coordinate activities across key stakeholder groups (e.g., risk functions), and facilitate decision-making.

Decentralized ← **Federated** → **Centralized**

Independent	Locally distributed	Balanced	Central + distributed	Centralized
				
Functional areas operate with complete autonomy, while maintaining global standards to meet specific enterprise requirements.	Functional areas control a majority of their business and technology operations, with some limited coordination from the enterprise to ensure objectives are achieved.	Responsibility and ownership are shared equally among the different functional areas and the enterprise.	The governance function provides a point of control and facilities decision-making, but functional areas own selective decisions and activities.	The governance function provides a single point of control and owns decision-making with functional areas having little or no responsibility.

Key considerations

- Align the governance structure to support the needs of the business and operations.
- Identify and incorporate key stakeholders across risk and compliance functions (e.g., compliance, legal, information security).
- Define clear roles and responsibilities across key stakeholders, including considering “lines of defense” model principles.

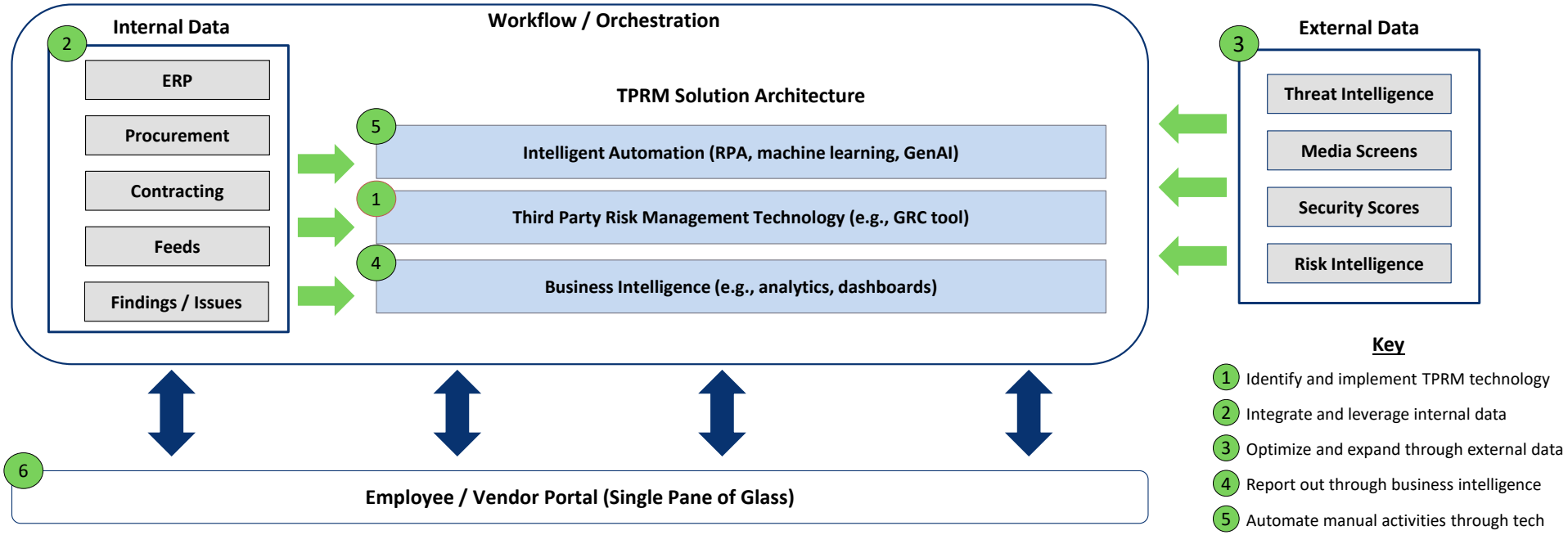
Overview of TPRM technology solution architecture

hfma
ma-ri chapter

NEW ENGLAND HEALTHCARE INTERNAL AUDITORS INC.

Overview of TPRM technology solution architecture

Moving from a current state of multiple, disparate technologies to a connected future state technology landscape is a common challenge organizations face; however, by identifying and driving to a connected target state, organizations can introduce innovative practices such as analytics and RPA.



1. Identify and implement TPRM / GRC technology

The following provides an overview of the TPRM technology landscape (which is not all-inclusive), including highlight various considerations:

Organizations need to consider a variety of factors when determining the appropriate technology solution(s) including:

1. Alignment to TPRM and tech roadmap
2. Functionality (aligned to target state requirements)
3. Cost of ownership
4. Integration with related areas (e.g., procurement, contracting, compliance)
5. User experience

	Procurement Systems	Enterprise GRC Systems	TPRM Specific Systems
Description	Technology platforms developed to support procurement activities (e.g., sourcing, purchasing, onboarding) that have started to provide select TPRM functionality.	Enterprise systems with multiple governance, risk management, and compliance use cases, including TPRM. Provides ability to automate and integrate risk activities across multiple areas, providing greater visibility to risks.	Smaller, boutique systems specifically developed for TPRM. These systems are often deployed to support a specific function (e.g., Cybersecurity). While select players are expanding into other areas, these platforms originated as TPRM platforms and do not offer broader use cases.
Example Players	SAP Ariba, Aravo	ServiceNow IRM, Archer, MetricStream	ProcessUnity, OneTrust
Considerations	¼ Procurement-focused functionality ¼ Integrations primarily aligned with ERP systems ¼ Procurement and supply chain focused ¼ Provides ability to integrate upfront procurement/supply chain activities with other areas ¼ Provides a view of sourcing, purchasing, and supply chain data combined with select risk data ¼ Procurement and supply chain functions often govern and define strategy for these systems	¼ Multiple GRC use cases, including TPRM ¼ Integrations consider internal and external data, including a variety of systems ¼ Transformation and user-experience focused ¼ Provides ability to connect activities and risk data across multiple areas and functions ¼ Provides a comprehensive view of risk and compliance due to breadth of use cases ¼ Multiple parties often involved in governing and defining the strategy for the system	¼ TPRM-focused functionality ¼ Integrations are primarily TPRM data focused ¼ TPRM or security focused as opposed to end-to-end transformation ¼ Provides ability to report on third party risks depending on the scope of risk areas ¼ Typically, managed and governed by a single or small number of parties ¼ Limits on integration with GRC and Procurement systems

2. Integrate and leverage internal data

The following graphic depicts an illustrative end-to-end TPRM process, including examples of typical stakeholders, systems, and data (master and transactional). Critical to understand and establish the solution and data architecture to simplify, scale, and orchestrate the process across multiple stakeholders.

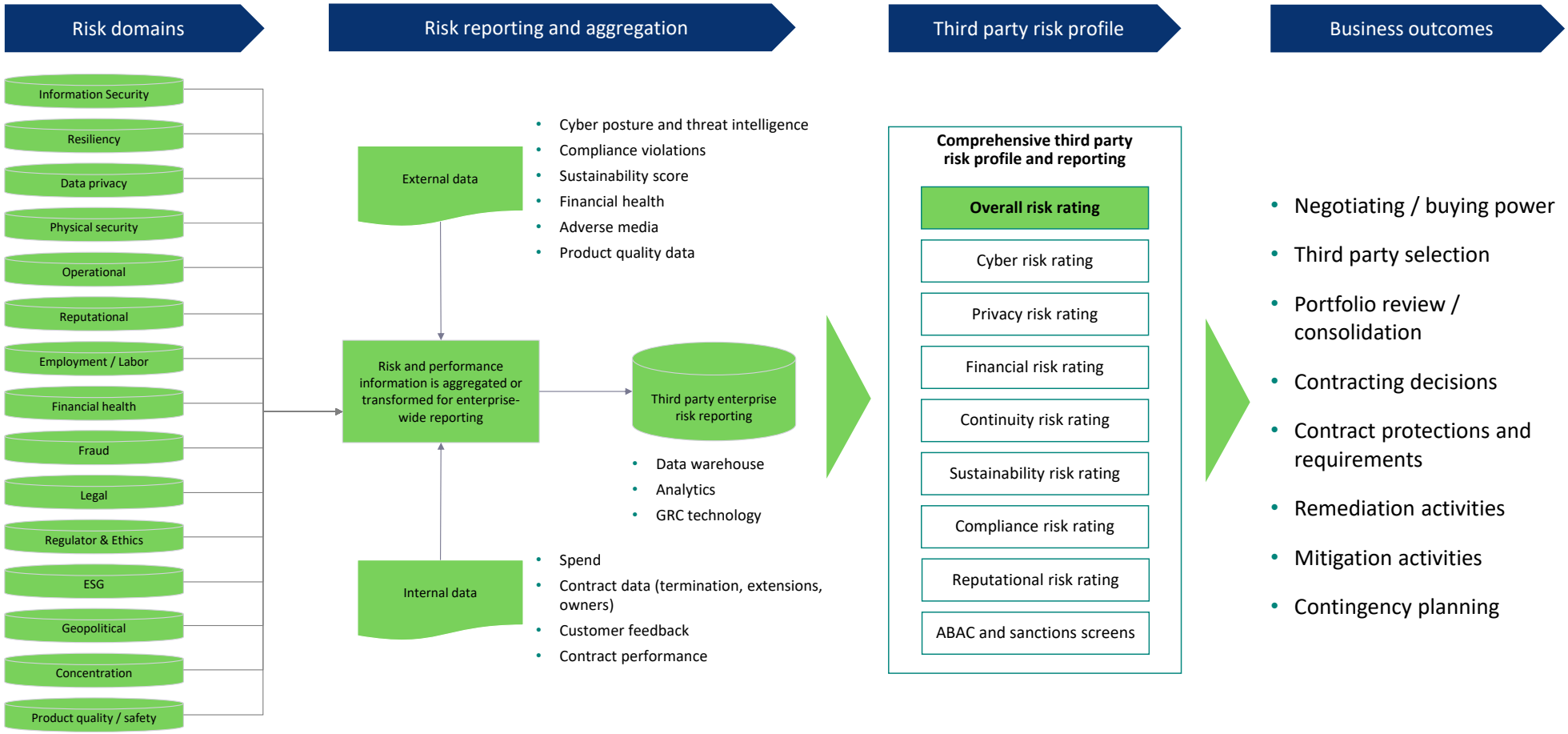
	1 Sourcing	2 Screening/ Risk Profiling	3 Due Diligence	4 Issue Management	5 Contracting	6 Onboarding	7 Management	8 Monitoring	9 Offboarding
Example Data	Third-Parties Services	Inherent Risk Questionnaires Inherent Risk Data External Risk Data Inherent Risk	Policies Controls Assessments Residual Risk	Issues	MSAs Contracts	Credentials Assets	Service Levels	Performance Spend External Risk Data Assessments	Offboarding Requests
Typical Systems	Sourcing/ERP	GRC Tech External Data Business Intelligence	GRC Tech Business Intelligence	GRC Tech Business Intelligence	Sourcing/ERP CLM	IAM Training	Sourcing/ERP Business Intelligence	Sourcing/ERP GRC Tech External Data Business Intelligence	IAM

3. Optimize and expand through external data

Implementation of external data can impact day-to-day operations and risk methodology to evaluate third party risk.

		Example
1 **Satisfy questionnaire-based assessments**	Leverage data to supplement questionnaire responses for full reliance on a specific domain	Information security questions supplemented with overall score from external data provider. Business continuity and privacy questions sent to third party for completion.
2 **Perform targeted assessments**	Analyze data to determine when targeted review is required based on predetermined thresholds	Financial health threshold is set at 7. If financial health score drops below a 7, perform detailed assessment.
3 **Initiate ad-hoc review**	Review alert-based notifications to determine action	Email alert received for data breach at ABC. Review cybersecurity rating to determine if in-depth assessment is required.
4 **Validate assessment responses**	Utilize data to confirm alignment with third party responses in questionnaire	Questionnaire response is that software patching is in place. Software patching rating is an 'F'. Third party response is not in alignment with data.
5 **Expand scope of risk domains**	Leverage data across domains not typically covered through the questionnaire-based assessment process	Geopolitical risk deemed in-scope for third party. Review geopolitical rating to understand risk level of the domain.
6 **Optimize assessment queue**	Leverage data to dynamically adjust assessment schedule to balance priority based on risk and anticipated deficiencies	Assessment for ABC third party is scheduled for July 2021. Information security rating drops from 'A' to 'D'. Assessment moved to March 2021.

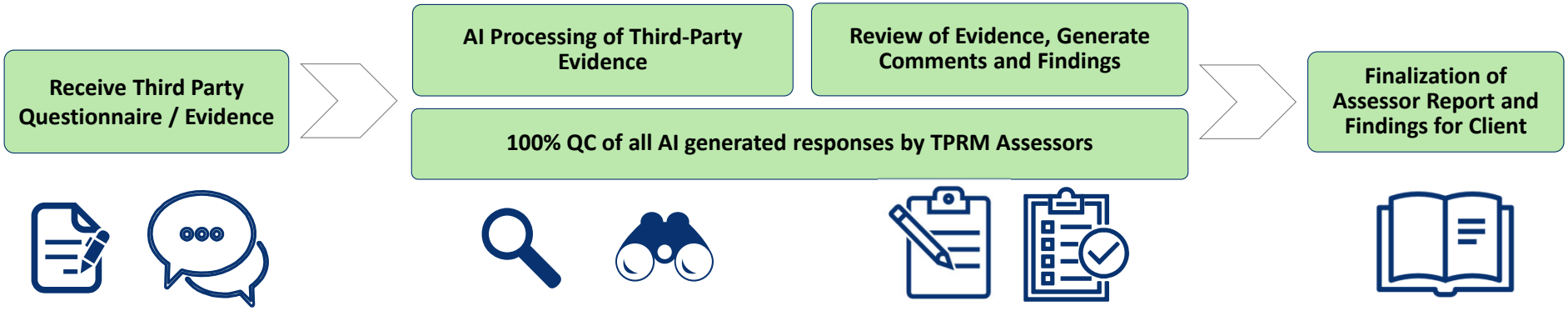
4. Report out through business intelligence



5. Automate manual activities through emerging tech

Leveraging AI/OCR/ML technology, there is the ability to improve assessment quality and reduce end-to-end timelines by automating the document review process generate draft comments and findings.

How to Leverage AI in TPRM



Benefits of TPRM Enabled by AI

Higher Assessment Quality leveraging the ability to scan entire document sets for accurate information and potential risks within third party control environments.

Faster end-to-end assessments with expedited processing of evidence and two levels of quality control across every assessment.

6. Establish single pane of glass

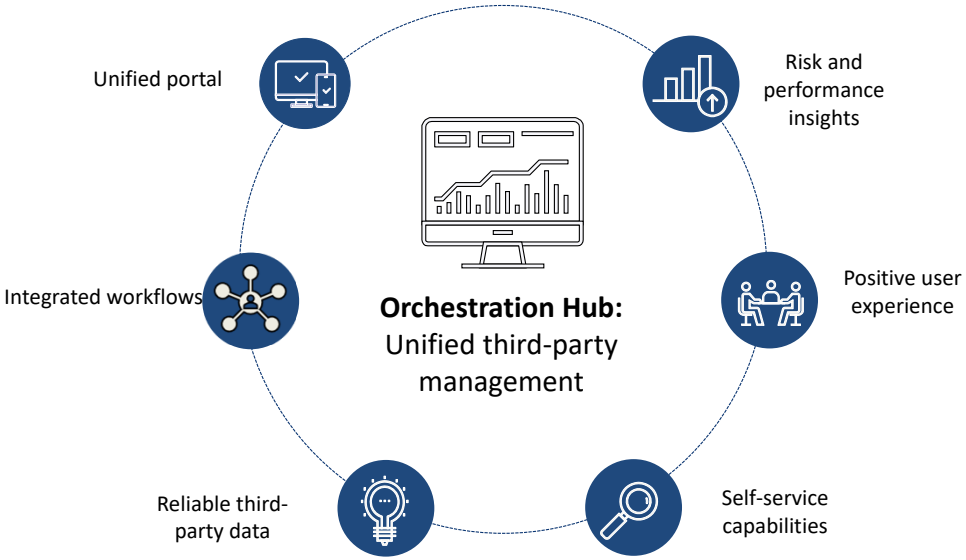
Significant opportunity exists to drive efficiencies, reduce risk, and enable growth by leveraging and Orchestration Hub to manage and digitize third-party risk management processes.

Current State

- Limited workflows - Multiple functions (e.g., Procurement, Cyber, Privacy, Legal, etc.) involved in third-party mgmt. with limited end-to-end workflows
- Disparate data - Third-party data is captured across multiple systems inhibiting efforts to manage monitor risk across the ecosystem
- Silos – Third-party risk is managed in silos with limited coordination
- Disconnected processes – Confusion as to where to handle different types of third-parties which may have different requirements (e.g., contingent workers, government, etc.)
- Disjointed user experience – Little automation and self-help, lack of ease regarding numerous portals and tools to navigate to per activity within the process
- Risk exposure – Risks may not be adequately covered depending on the third-party type (e.g., cyber, resiliency, reputational, regulatory, ESG)

Target State

Connected processes and data to effectively and efficiently manage third-party ecosystems



Actioning these key topics through roadmap development

hfma
ma-ri chapter

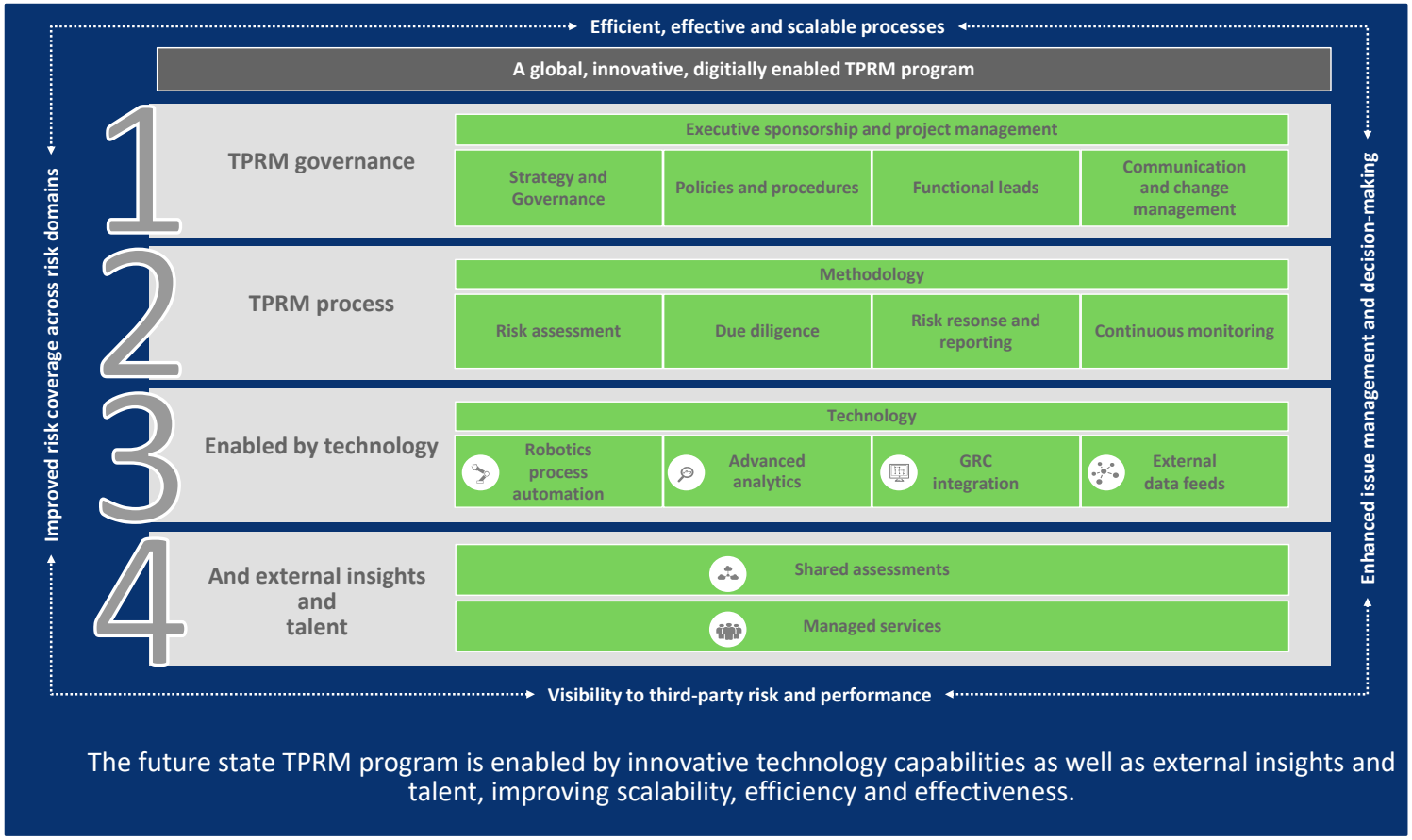
NEW ENGLAND HEALTHCARE INTERNAL AUDITORS INC.

Roadmap to successful TPRM program

What does your future state TPRM program look like?

How does your roadmap support your future state vision and priorities?

How does your program fit into the broader aspects of third-party management?



QUESTIONS

hfma
ma-ri chapter