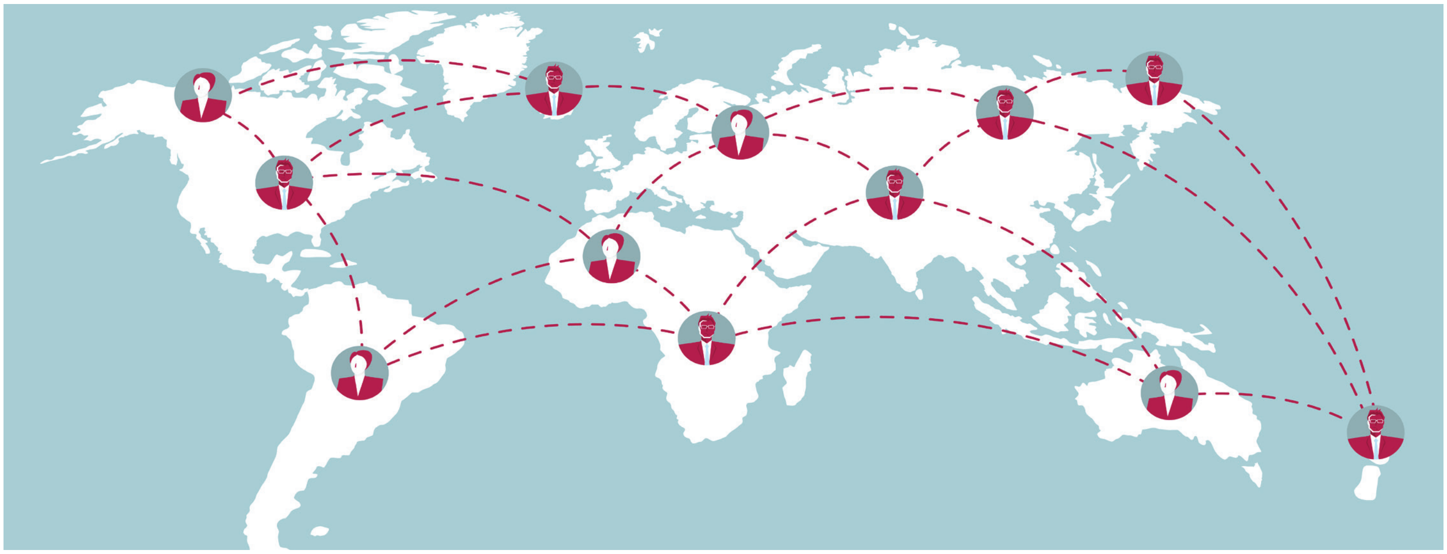
Point of View

GENPACT
GENERATING IMPACT℠

GENERATING **RISK AND COMPLIANCE** IMPACT

The coming regulatory wave: Vendor risk management



A compliance risk is looming, and most businesses are not yet ready for it. With CXOs focused on many burning issues, vendor risk management (VRM) has not been a priority beyond attention to price and quality. That needs to change, and quickly, because the regulators—and the related enforcement bodies—are becoming more aggressive.

Every CXO understands the need to manage vendors to control costs and ensure quality goods and services. A single bad vendor can have catastrophic impact. For example, a defect in a critical item supplied to an oil rig resulted in lasting damage to the oil company, vendor, economy, and environment.

What many executives do not realize is that VRM has become the focus of increasing interest by regulatory agencies and their respective enforcement ecosystems. Multiple laws and agencies such as the Office of the Comptroller of the Currency (OCC), the Health Insurance Portability and Accountability Act (HIPAA), the Consumer Financial Protection Bureau (CFPB), the Foreign Corrupt Practices Act (FCPA), Dodd–Frank, the HITECH Act, and the Gramm-Leach-Bliley Act require enterprises to set up a robust VRM framework.

This focus on VRM compliance has caught many organizations off-guard. Most are unknowingly at high risk of spending inordinate amounts of time fixing deficiencies instead of addressing business goals, with a potential impact on the bottom line from regulatory losses. And that's on top of the damage arising from poor VRM in general.

What regulators will expect of VRM programs

Many large businesses are already discovering that their systems and processes related to VRM are simply not adequate from a purely business standpoint. One leading automobile manufacturer saw its stock price fall by 15% and its net profit affected by $2 billion in lost sales and output when faulty parts procured in part from vendors resulted in the recall of nine million cars. A major sportswear brand and a popular consumer electronics company experienced significant earnings dips and a huge loss of reputation when unfair and unsafe workplace environments and practices at key vendors were exposed, creating negative public perception of the companies' brands.

These are exactly the things regulators will be looking at. Unfortunately, many CXOs are reluctant to divert their attention from other pressing challenges to deal with an issue that may not be impacting them right now. However, businesses need to prepare for the coming VRM regulatory offensive. Regulators will expect more robust vendor risk management frameworks and ongoing monitoring of vendors, including proof of vendor oversight, audits, surveys, and close management of a company's thousands of vendors, large and small.

A faster road to compliant VRM

Currently, there is no standard approach to meeting the regulatory requirements for VRM. Companies are developing their own programs, when in fact a cooperative effort to establish a single standard would be beneficial for all involved. Supplier Ethical Data Exchange is a good example of how businesses within an industry could build shared VRM data exchanges that vet vendors and update performance data with the information readily accessible to participating companies.

In the interim, implementing a robust VRM operating model can be achieved relatively quickly through a focused, risk-based framework of better processes, analytics, and monitoring mechanisms to run the respective operations cost effectively. Better technology is critical, since screening and assessing performance for tens of thousands of vendors worldwide requires the ability to filter massive amounts of data quickly and accurately. Manual processes and Excel spreadsheets are inadequate for this task, and although some off-the-shelf tools can help, none were specifically designed for VRM. Companies must therefore either adapt the tools to business needs, design internal systems for VRM, or leverage third-party expertise. The best tools are platform agnostic, able to pull data from any legacy system and quickly present a coherent view of every vendor across the enterprise. Integrating databases such as Lexis Nexis, Dow Jones and Thomson Reuters with a technology platform suitable for VRM can lower risk by identifying the riskiness of the vendor at the onboarding stage and flagging any negative feedback.

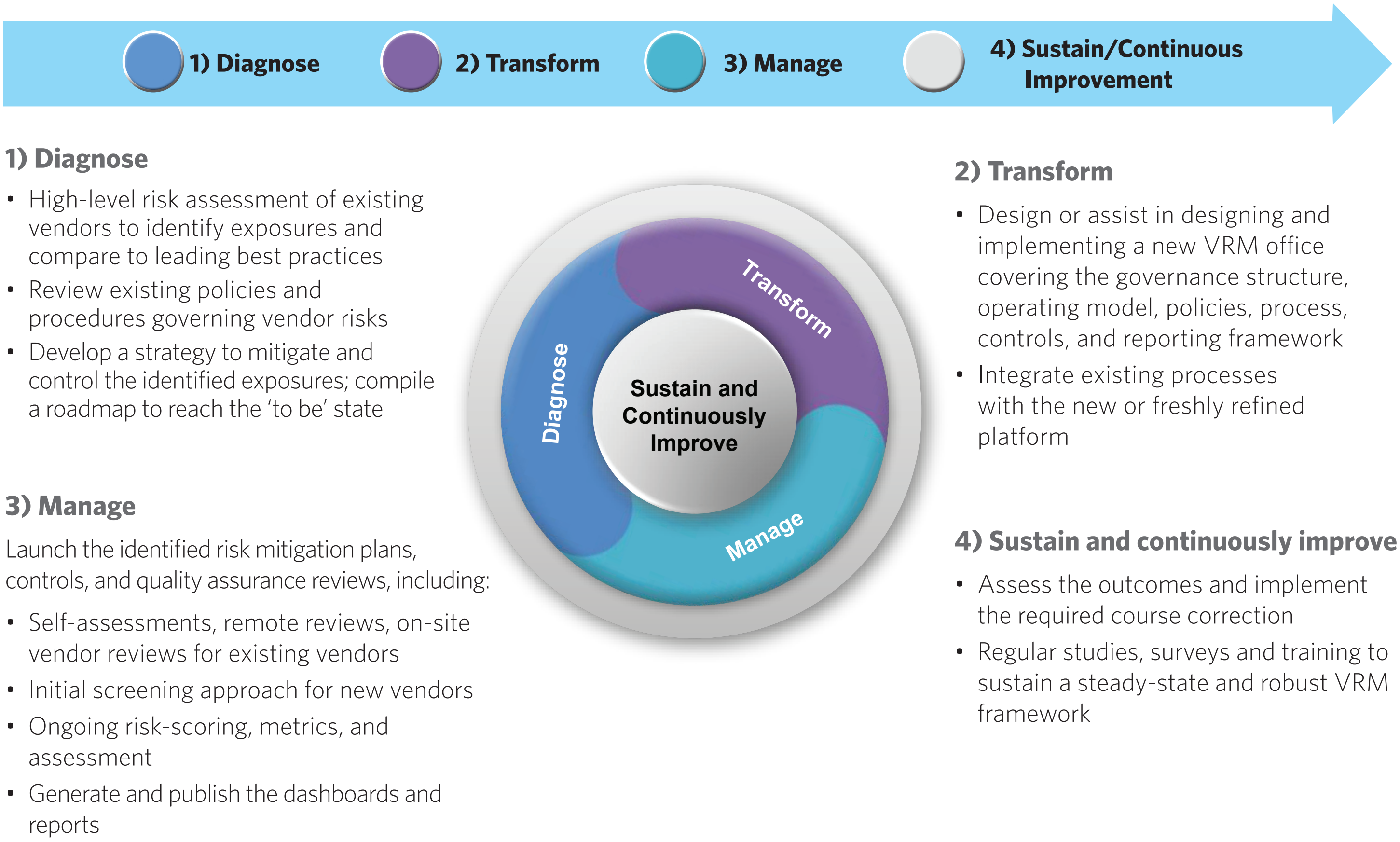
> ***Businesses need to prepare for the coming VRM regulatory offensive***

Better technologies support more effective VRM processes, and the compiled data supports analytics capable of spotting overpricing, poor performance, and other enterprise risks. It is crucial to not only continuously track vendor performance with a carefully chosen set of appropriate metrics but to also use the results to refine the VRM program. Analyzing the data is not enough; it must be applied on an ongoing basis to weed out risky vendors and keep up with regulatory changes.

An experienced partner can provide the required analytics tools and quickly conduct a full-coverage screening of the company's vendors to achieve a clean vendor database free from multiple or non-standard contracts. This results in a fully vetted set of reliable vendors that won't put business continuity or brand value at risk. The new mechanisms put in place for ongoing vendor assessment can ensure continuing high performance and best pricing. This integrated framework produces a multitude of high-impact benefits, including the following:

1. Moving VRM processes toward best in class, reducing the risk of non-compliance as well as other security, pricing, and quality issues that could impact the brand and profitability
2. Enabling the company to demonstrate at any time how it manages its vendors, to whatever level of detail is required by regulators
3. Freeing executive management to focus on critical business needs and goals rather than corrective actions

Companies should initiate structured risk assessments to understand the effort required for ongoing VRM monitoring and then decide what they can manage through internal resources and where they are likely to require external partners to support and manage their processes.


1) Diagnose
2) Transform
3) Manage
4) Sustain/Continuous Improvement
Transform
Diagnose
Sustain and Continuously Improve
Manage

1) Diagnose

- High-level risk assessment of existing vendors to identify exposures and compare to leading best practices
- Review existing policies and procedures governing vendor risks
- Develop a strategy to mitigate and control the identified exposures; compile a roadmap to reach the 'to be' state

2) Transform

- Design or assist in designing and implementing a new VRM office covering the governance structure, operating model, policies, process, controls, and reporting framework
- Integrate existing processes with the new or freshly refined platform

3) Manage

Launch the identified risk mitigation plans, controls, and quality assurance reviews, including:

- Self-assessments, remote reviews, on-site vendor reviews for existing vendors
- Initial screening approach for new vendors
- Ongoing risk-scoring, metrics, and assessment
- Generate and publish the dashboards and reports

4) Sustain and continuously improve

- Assess the outcomes and implement the required course correction
- Regular studies, surveys and training to sustain a steady-state and robust VRM framework

Figure 1: Four steps required to achieve and sustain effective VRM

An ounce of prevention is worth a pound of penalties

Although the news features VRM horror stories, such as the multinational food manufacturer that suffered a huge loss of brand appeal and sales thanks to an unappetizing smell coming from the packaging, better tools and processes for assessing risk and managing vendor relationships can prevent these woes. The returns are wide-ranging. For instance, a large US conglomerate's financial services division was subject to regulatory oversight.

Partnering with a third-party vendor, the company attained a solid risk assessment framework, effective monitoring tools, workflows, and policies that enabled near real-time approval from regulators. This kept consumer and stakeholder confidence in the brand high, and freed managers and staff from onerous, time-consuming rework and re-inspections, allowing them to concentrate on driving business value.

Vendor risk management will become a major target of regulatory oversight, which means the appropriate VRM program must be comprehensive. A viable program needs to encompass quality, performance, financial, and non-financial (reputational) risk, and must be integrated across the enterprise rather than siloed in each department.

The long-term gains of strengthening VRM are worth the short-term effort. This will prove especially true when the regulators' scrutiny increases. Proven advanced operating models can achieve good VRM within a reasonable time, in relatively non-intrusive ways. The time to start is now.

This paper was authored by Subhashis Nath, Global Senior Partner for Corporate Governance and Controllership Solutioning, Genpact.