Gartner

Stay Ahead of Growing Third-Party Risk

Edited by Chris Audet
Director, Gartner

Introduction

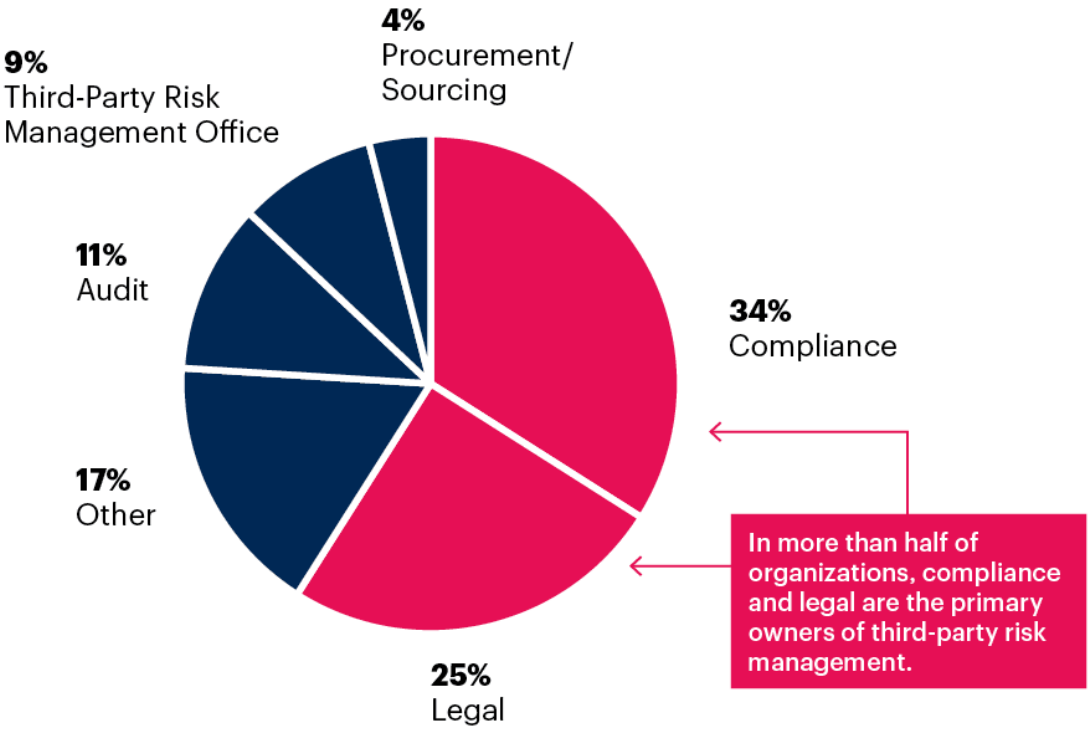
“There's no question that third parties are redefining how our business competes in the new digital world,” said one chief compliance officer at a financial services organization.

Today's third parties require more access to the organization's data assets and are increasingly working with their own third parties, multiplying the size and complexity of the third-party network. In fact, in the last four years, legal and compliance leaders have classified 2.5X more third parties as high-risk.

Managing the risks associated with these networks while not hindering business speed is a critical challenge for leaders.

Managing Third-Party Risk

Primary Functional Owner of Third-Party Risk Management



n = 256 legal and compliance leaders

Source: 2019 Gartner Third-Party Risk Management Model

A Cross-Functional Concern

Compliance and legal are the primary owners of third-party risk management but many other functions have a stake in improving risk management and business outcomes.

Third-Party Risks Are Changing

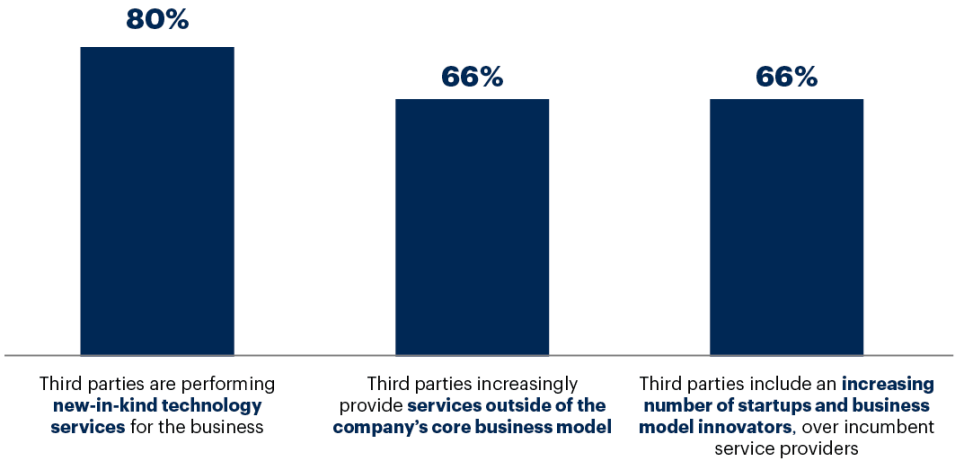
This year, twice as many compliance leaders identify third-party risk as a top threat. This is because third-party risks have fundamentally changed. Leaders say they have experienced:

- Greater variability in the maturity of their third-party network
- Third parties working with an increasing number of third parties themselves
- Increased third-party access to organizational data assets

> **"Consider the new ways your own business is using third parties. Increasingly, they're performing new-in-kind technology or analytics services, providing services outside of the company's core business model, and are increasingly comprised of startups and other business model innovators. These changes demand a fundamentally different approach to risk identification and monitoring."**
> Chris Audet, Director, Gartner Research & Advisory

We're Using Third Parties in New Ways

Role of Third Parties in Our Business
Percentage of Legal and Compliance Leaders Agreeing With Each Statement



n = 256 legal and compliance leaders
Source: 2019 Gartner Third-Party Risk Management Model

Not only that, the role third parties play in business is also changing.

Leaders find themselves in the middle of what feels like an unwinnable war: one that demands risk oversight while maintaining speed.

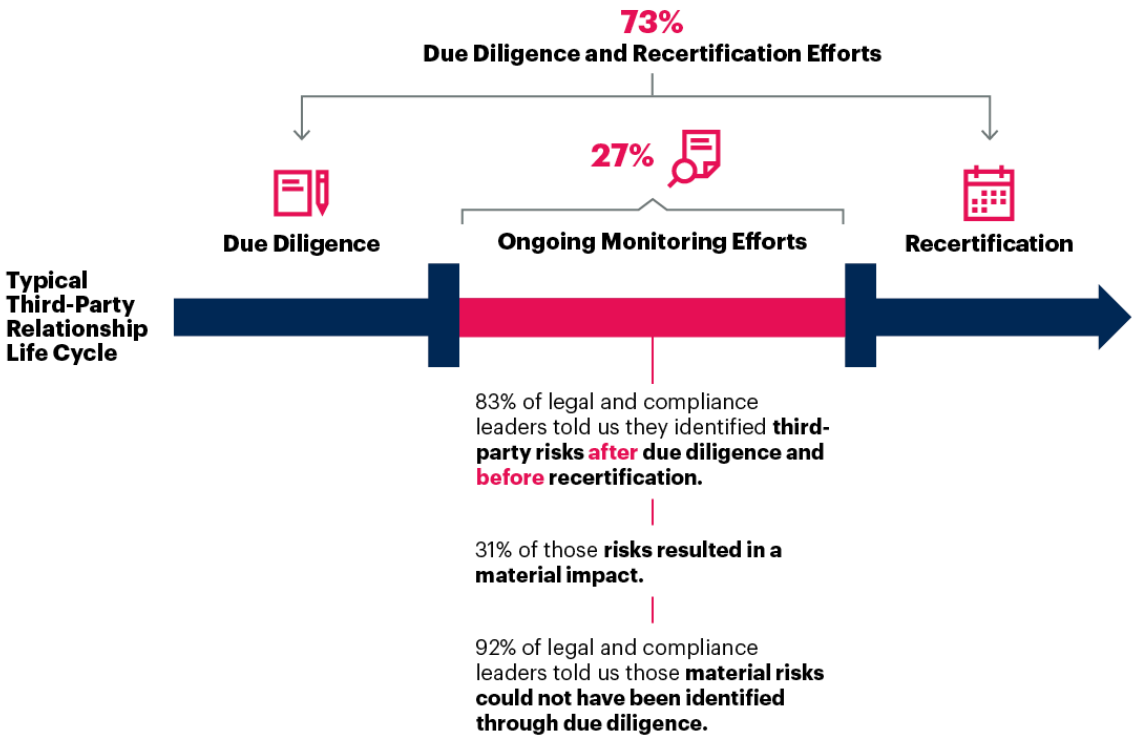
The Current Approach Is Point-in-Time-Focused

Traditionally, 73% of effort devoted to risk identification is allocated to due diligence and recertification efforts, with only 27% of effort allocated to identifying risks over the course of the relationship.

Traditional Point-in-Time Approach

Effort Allocated to Identifying and Monitoring Third-Party Risks

Percentage of Effort Legal and Compliance Leaders Allocate to Third-Party Risk Activities



n = 256 legal and compliance leaders

Source: 2019 Gartner Third-Party Risk Management Model

Why Point-in-Time?

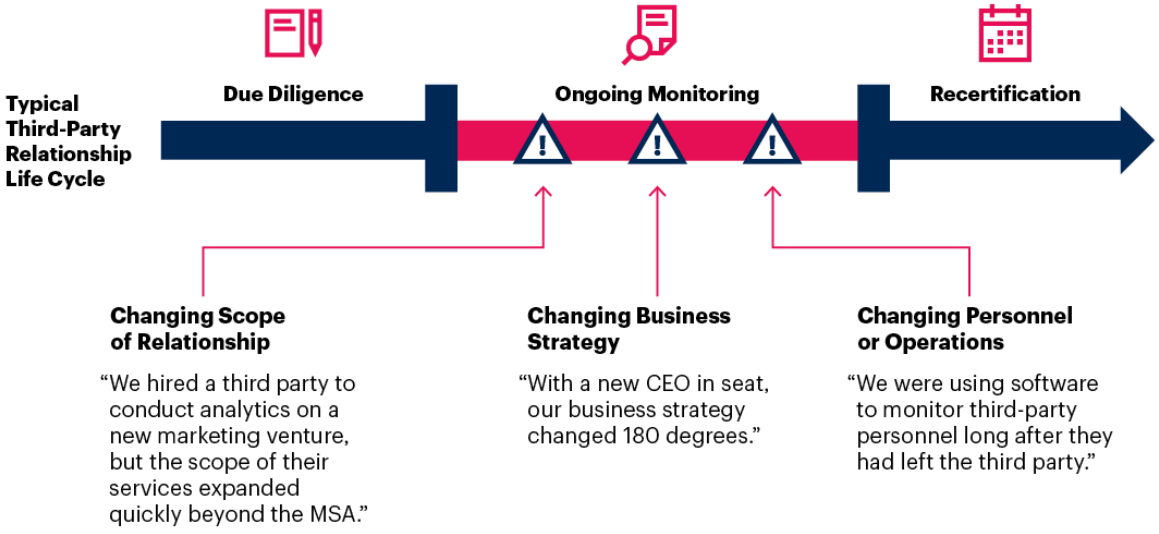
- Mandates from regulators and enforcement bodies
- Expectations from consumers and an activist media
- Cost implications

The point-in-time approach often fails because it misses changes in third-party relationships

The current monitoring approach cannot account for changes that are inevitable in conducting business today — those associated with strategy, personnel, risk appetite or scope of relationship.

Point-in-Time Misses Ongoing Changes in the Relationship

Changes Affecting Third-Party Risks After Due Diligence and Before Recertification



n = 256 legal and compliance leaders

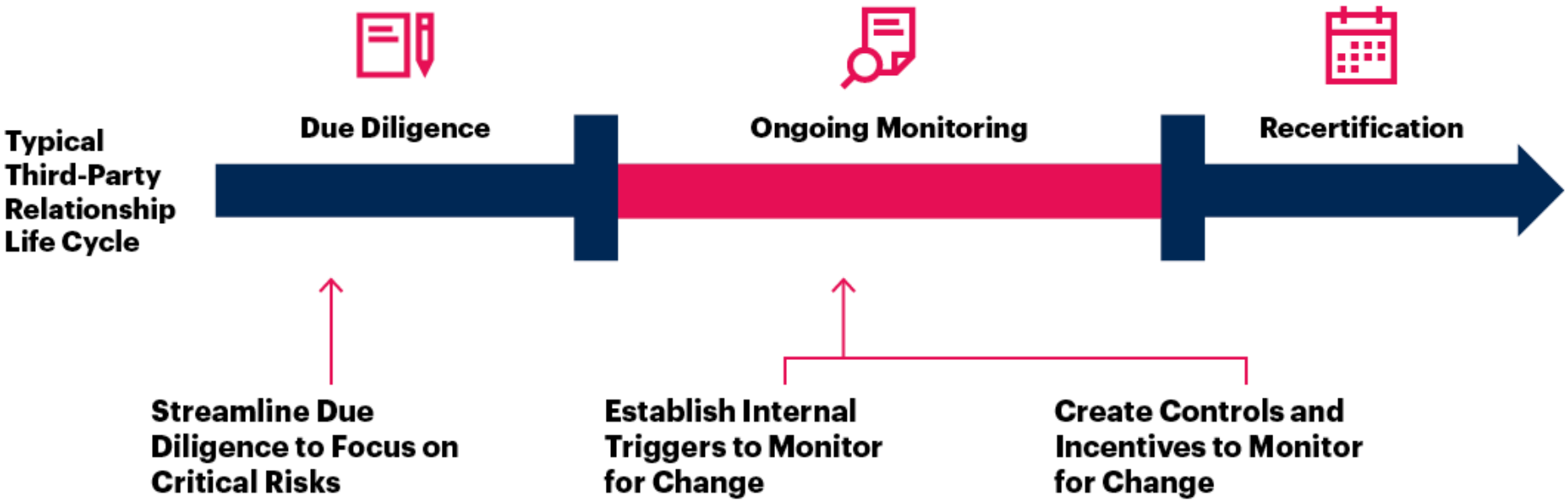
Source: 2019 Gartner Third-Party Risk Management Model

Make the Shift to an Iterative Approach

Gartner research found that to improve the identification and monitoring of third-party risk, legal and compliance leaders should take an iterative approach. This approach requires some information to be learned prior to contracting with the third party, but places greater emphasis on continued learning over the course of the third-party relationship.

Next Steps for the Iterative Approach

Implement an Iterative Approach to Third-Party Risk Identification and Monitoring



n = 256 legal and compliance leaders

Source: 2019 Gartner Third-Party Risk Management Model

Streamline Due Diligence to Focus on Critical Risks

Use a data-driven methodology to determine risks that have impacted the organization in the past and source feedback from the business to identify future risks.

Case Study: Data-Driven Due Diligence Questionnaire

Facing an ever-expanding due diligence questionnaire and lengthy due diligence process, a healthcare organization sought to reduce its time and effort on due diligence. This data-driven understanding focuses on risks that have previously impacted the company or may impact it in the future. The compliance team assessed which due diligence questions have been the most effective indicators of risk based upon previous third-party incidents, industry data, and relevant hotline data (among other sources).

Data-Driven Analysis to Identify Critical Questions

Process to Determine Critical Due Diligence Questions
Illustrative

To determine critical due diligence questions, compliance first asks what questions are required based on relevant laws and regulation. Second, what questions capture **risks that have impacted our organization in the past (or impacted others within the industry)?**

Step 1: Determine Critical Questions

What information is critical for our company to learn about before engaging with a third party based on **risks that have impacted our organization in the past?**

Review existing data sources to understand past and current third-party risk incidents or potential risk incidents: previous quarterly risk reports from internal audit, hotline data reports and others.

Step 2: Review Multiple Data Sources

- **Government Settlements (Quarterly Review)**
- **Industry Association Quarterly Risk Reports**
- **Quarterly Risk Report (ERM and Compliance)**
- **1Q19 Hotline Report**

Establish Internal Triggers to Monitor for Change

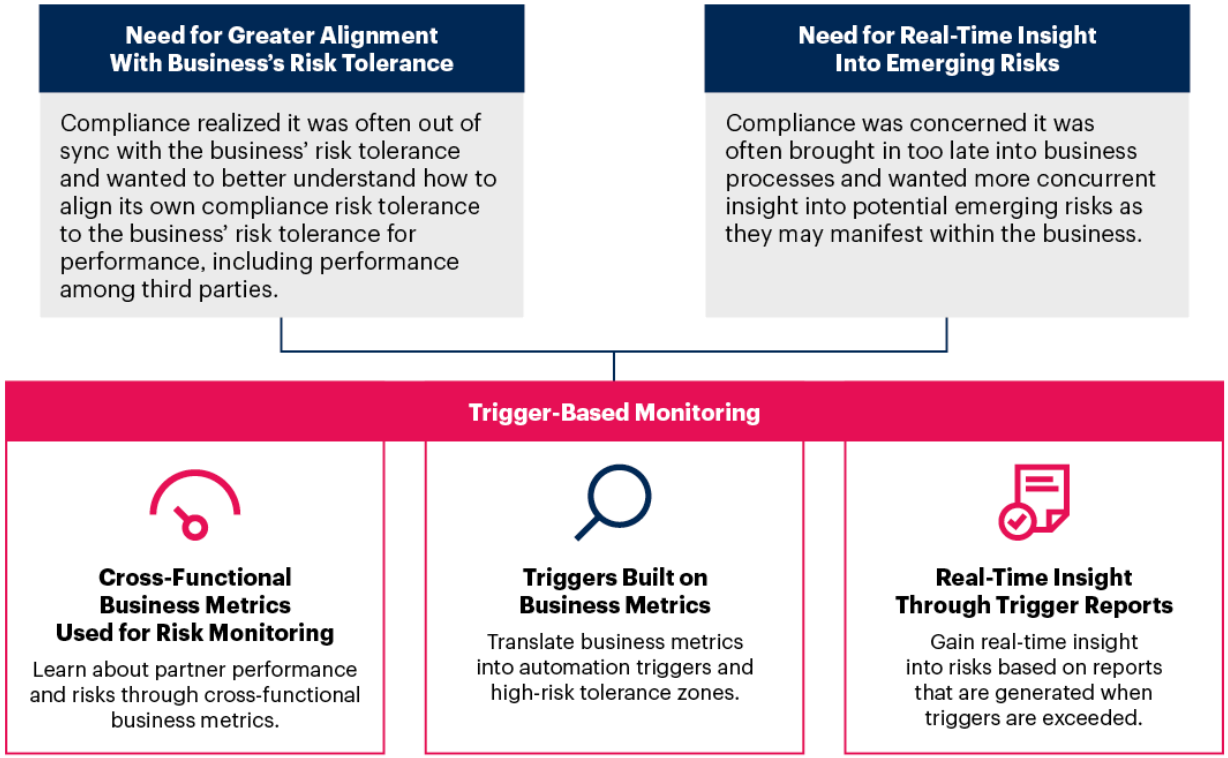
Monitor your third-party network with triggers throughout the business to signal changes in the third-party relationship.

Case Study: Trigger-Based Monitoring

A financial services organization wanted a more comprehensive means of reviewing operations across the business to identify activity that could expose the company to risk. The organization built automated trigger reports to identify emerging risks based on an understanding of cross-functional business metrics. When observed metrics are exceeded, a report is triggered for compliance review, alerting compliance to an emerging risk in real-time.

The Drivers of Trigger-Based Monitoring

Two Primary Drivers for Trigger-Based Monitoring



Create Controls and Incentives to Monitor for Change

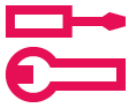
Embed controls and incentives to manage high-risk third parties and improve ongoing monitoring.

Case Study: Collaborative Risk Management

An organization providing telecommunications services faced two distinct challenges. First, suppliers had an uneven level of understanding of how to tackle reputation risks posed by their suppliers. Second, it was difficult to assess the capability of data collected during traditional ethical and environmental risk audits.

To overcome these challenges, the organization must:

Empower strategic suppliers to own reputation risk–management across their supply network. Create shared urgency around managing reputation risks across an extended supply base by convening on-site visits and workshops for strategic suppliers that focus on building the business case for collaborative risk management.



Equip suppliers with tools to ensure a consistent approach to assessing the supply base. Replace checklist approaches to evaluating suppliers with tools that allow strategic suppliers to cross-reference information from multiple sources and thus obtain a more credible evaluation.

Three Key Shifts for Legal and Compliance Leaders

1. Streamline due diligence to focus on critical risks

Identify opportunities to reduce exhaustive due diligence and streamline processes with a focus on critical risks.

2. Establish internal triggers to monitor for change

Monitor your third-party network with triggers throughout the business to signal changes in the third-party relationship.

3. Create controls and incentives to monitor for change

Embed controls and incentives to manage high-risk third parties and improve ongoing monitoring.

An Iterative Approach Improves Outcomes

An interative approach has a positive impact on desired risk management and business outcomes.

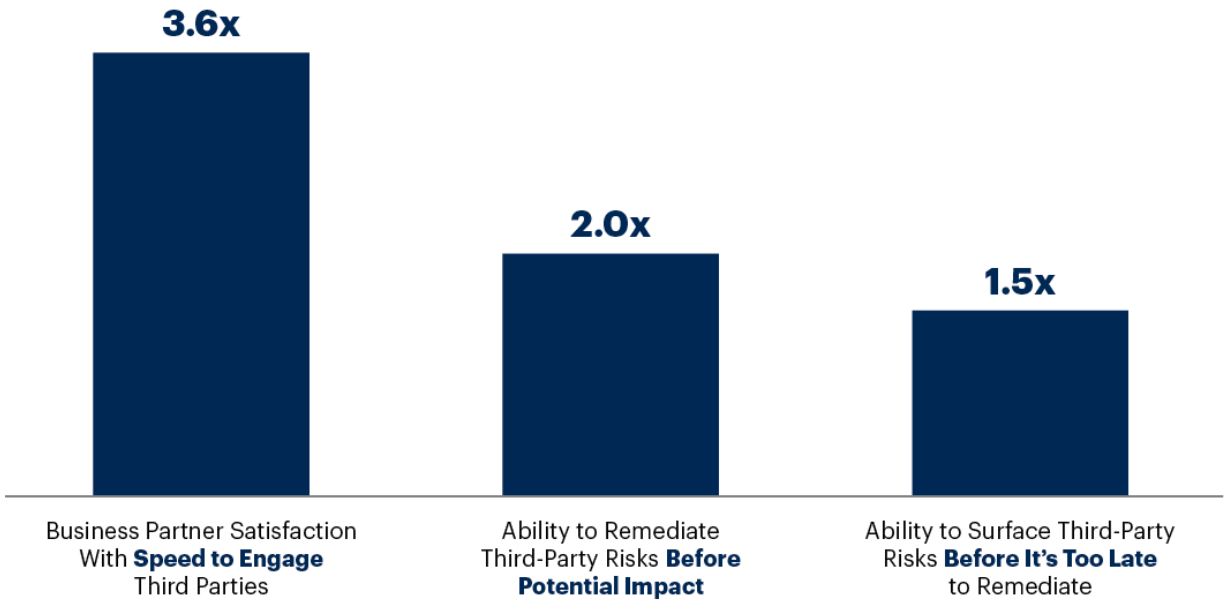
Improved Outcomes

Through this approach, leaders will see improved outcomes, including the:

- Ability to surface third-party risks before it's too late to remediate
- Ability to quickly remediate third-party risks before they have any material impact
- Satisfaction of business partners when it comes to the speed of due diligence, onboarding and engaging with third parties

An Iterative Approach Improves Outcomes

Impact of the Iterative Approach on Risk and Business Outcomes
Percentage Improvement in Desired Outcomes as a Result of Moving From 25th to 75th Percentile



n = 256 legal and compliance leaders
Source: 2019 Gartner Third-Party Risk Management Model

Learn more.
Dig deep.
Stay ahead.

Gartner for Legal & Compliance Leaders provides research insights, advice, tools and data to address mission-critical priorities and keep up with the accelerating pace of business today.
On the web, visit:
gartner.com/en/legal-compliance