# Closing Gaps in Third-Party Risk Management – Defining a Larger Role for Internal Audit

Jan. 15, 2014

# Agenda

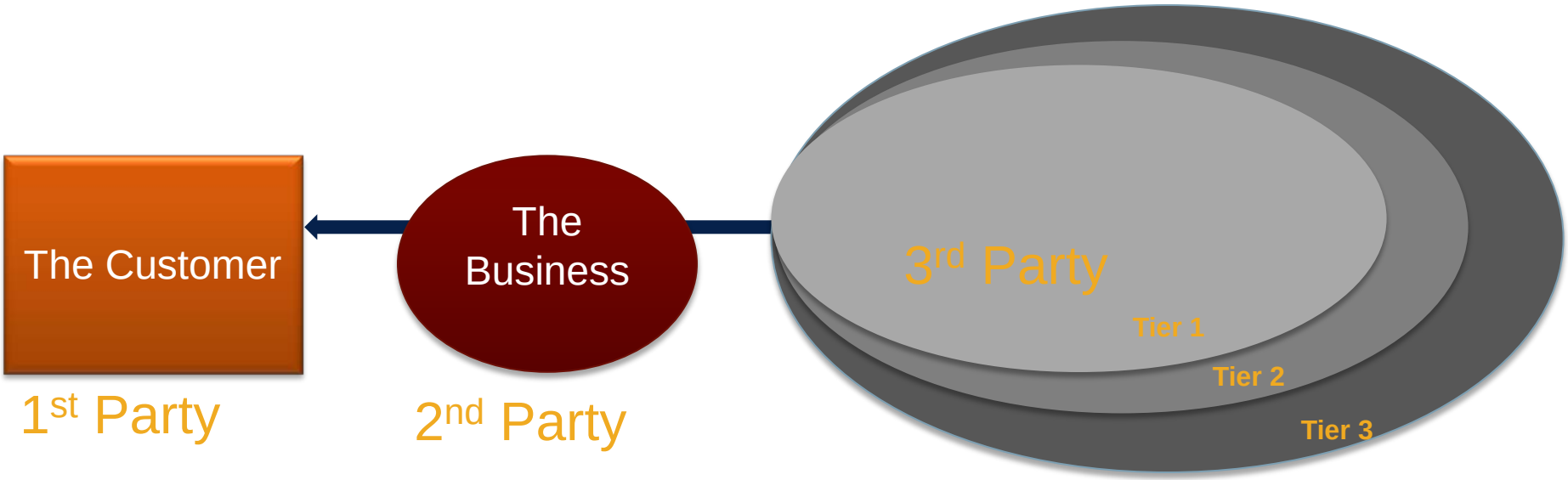
- Background on Third-Parties
- Regulatory Developments
- The Business Case for Improving Third Party Risk Management
- Internal Audit's Role
- Case Studies
- Tools for the Field

# The Four Principles of the New Internal Audit Model

# Polling Question 1

- Which area of the New Internal Audit Model is getting the most attention at your organization in this calendar year
  - A. Compliance
  - B. Assurance
  - C. Risk Identification
  - D. Performance Improvement
  - E. Unsure/don't know

# Third Parties



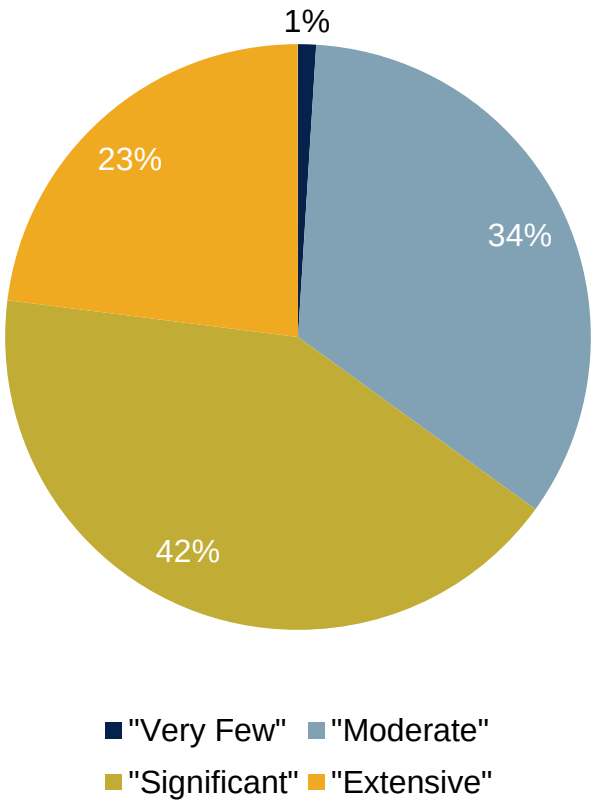
# Regulations in the Headlines

- FCPA
- U.K. Anti-Bribery Act
- Conflict Minerals (Dodd-Frank)
- *California Transparency in Supply Chains Act of 2010*

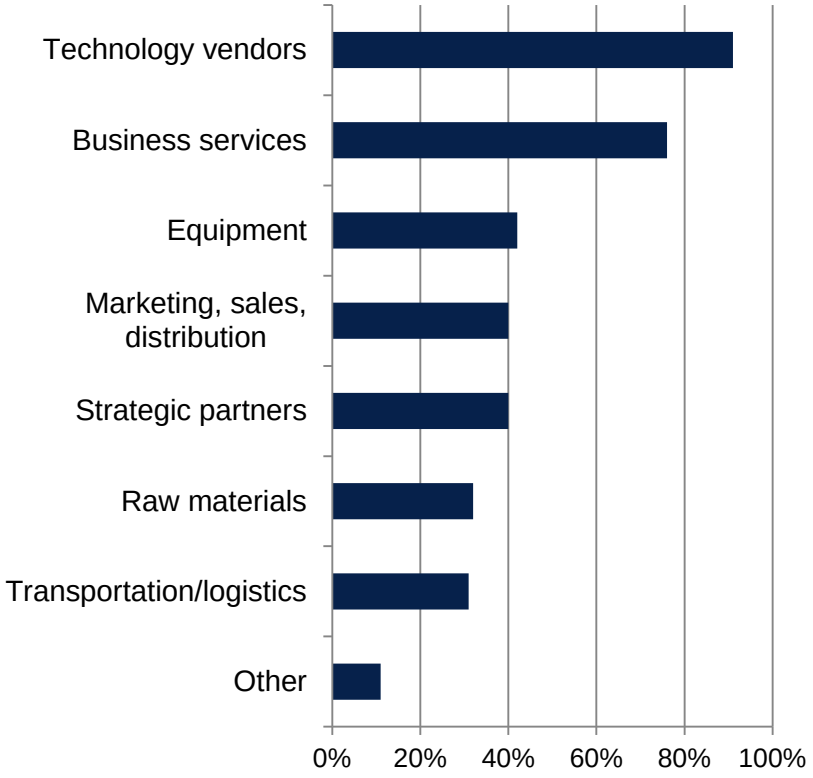
- OCC – Third-Party Relationships (10/30/13)
- FDIC
- FFIEC

# Trends in the Use of Third Parties Across the Business

**Use of Third Parties**

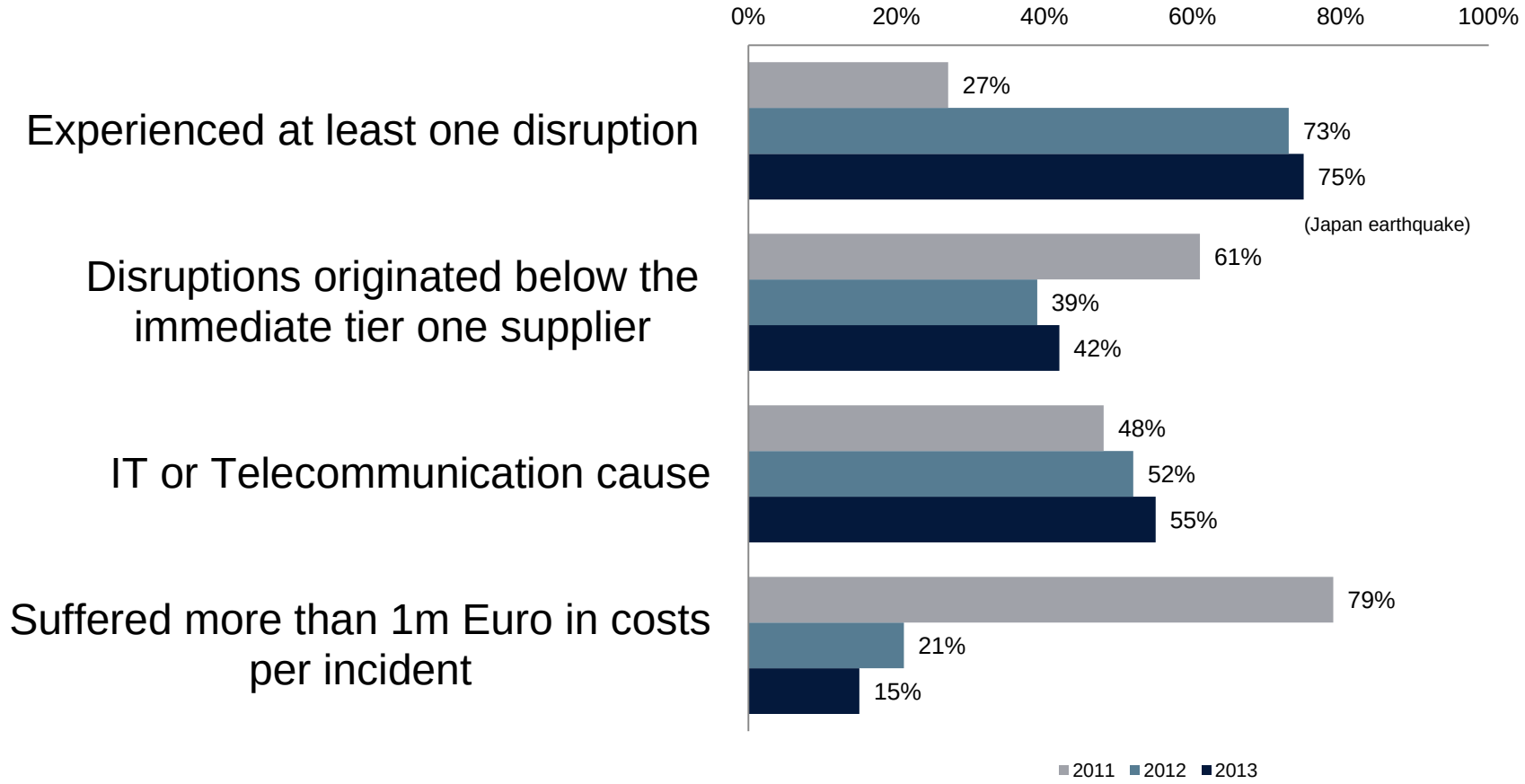



**Which types of third parties are significant in your business model?**



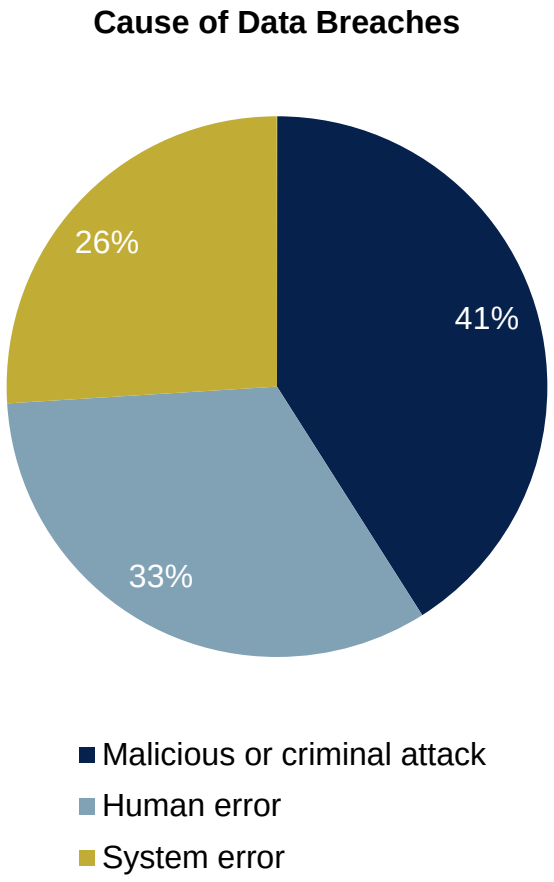

Source:"Closing the Gaps in Third-Party Risk Management, Defining a Larger Role for Internal Audit," December 2013, Sponsored by Crowe Horwath LLP

# The Business Case for Investing in Third-Party Risk Management: Supply Disruptions




Source: "Supply Chain Resilience," November 2012 and November 2013, Business Continuity Institute

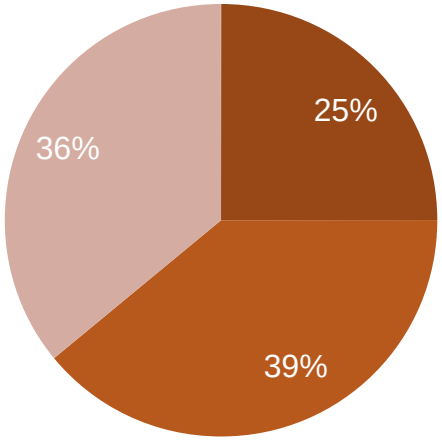
# The Business Case for Investing in Third-Party Risk Management: Data Breaches




Source: "2013 Cost of Data Breach Study: Global Analysis", Sponsored by Symantec, May 2013, Ponemon Institute

# Monitoring Frequency and Origin of Disruption

**Do you record, measure, and report on performance-affecting supply chain disruptions?**

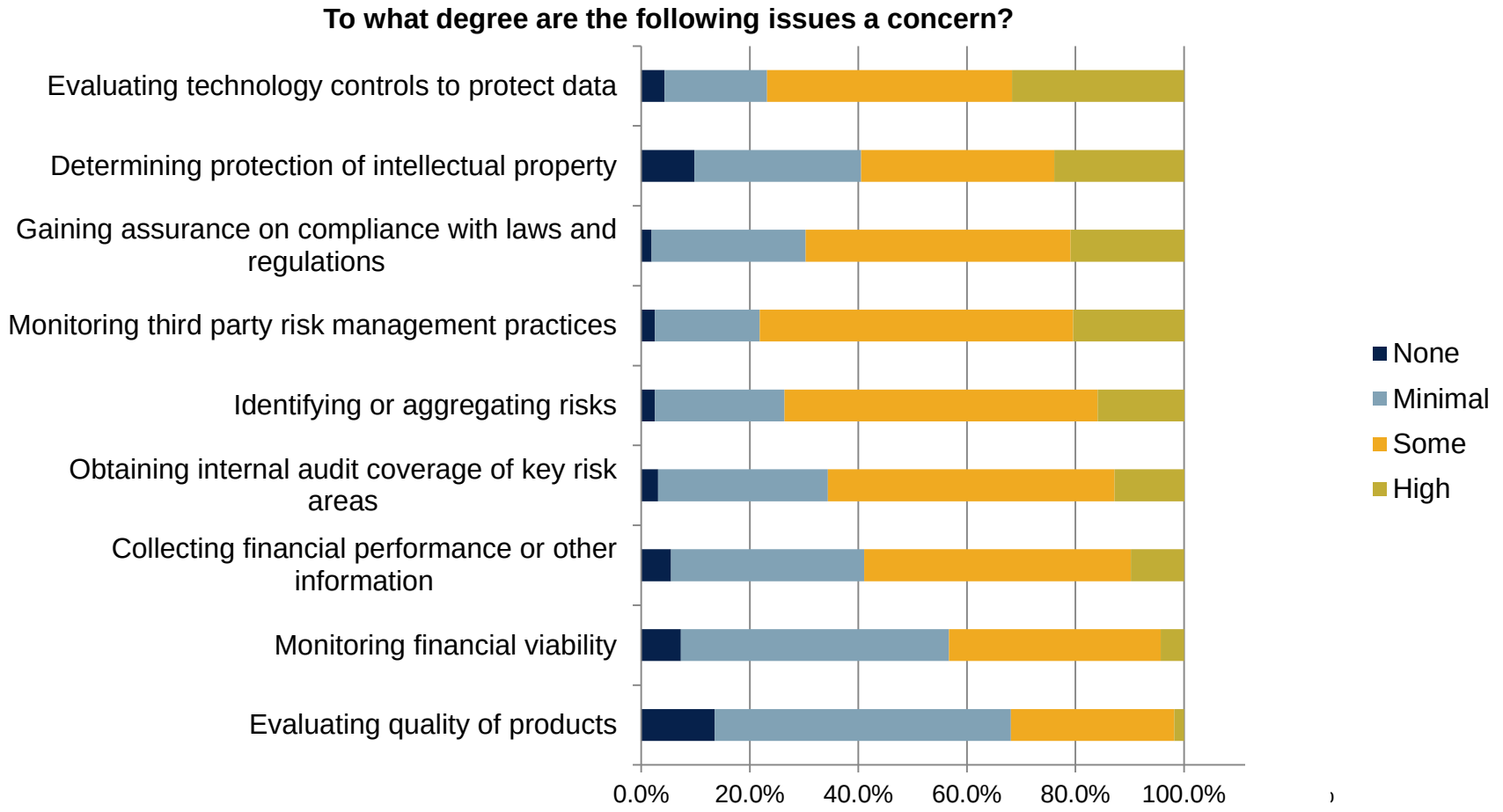



**(i.e. where an unplanned cost has been incurred or loss of productivity or revenue experienced)?**

- Coordinated and reported across the enterprise
- Not aggregated, but managed within certain departments/functions
- No

Source: "Supply Chain Resilience 2013," November 2013, Business Continuity Institute

# Third-Party Risk Management Concerns

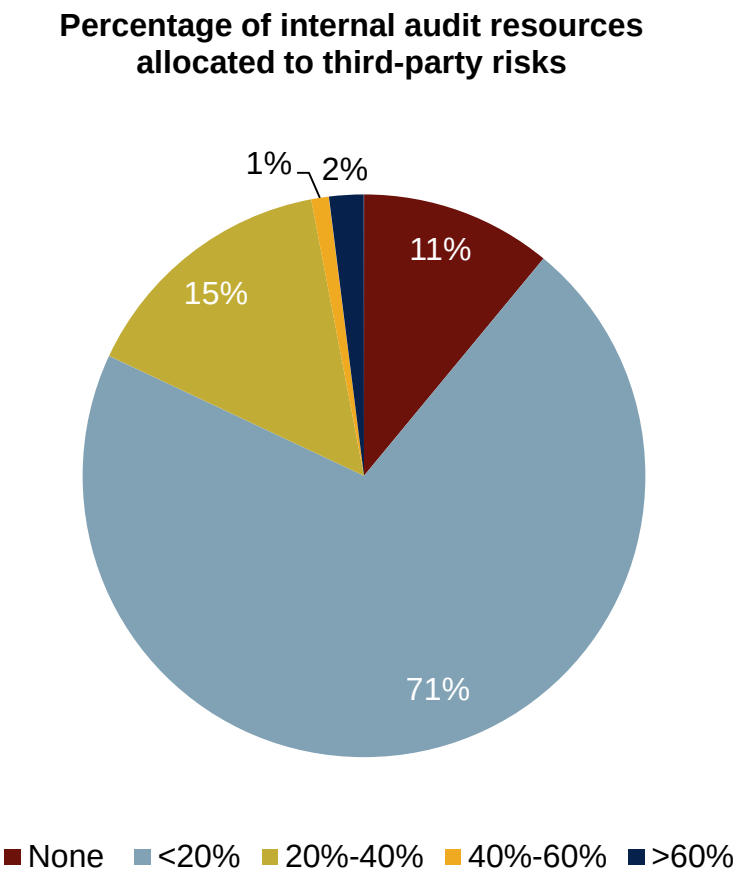



Source: "Closing the Gaps in Third-Party Risk Management, Defining a Larger Role for Internal Audit," December 2013, Sponsored by Crowe Horwath LLP

# Polling Question 2

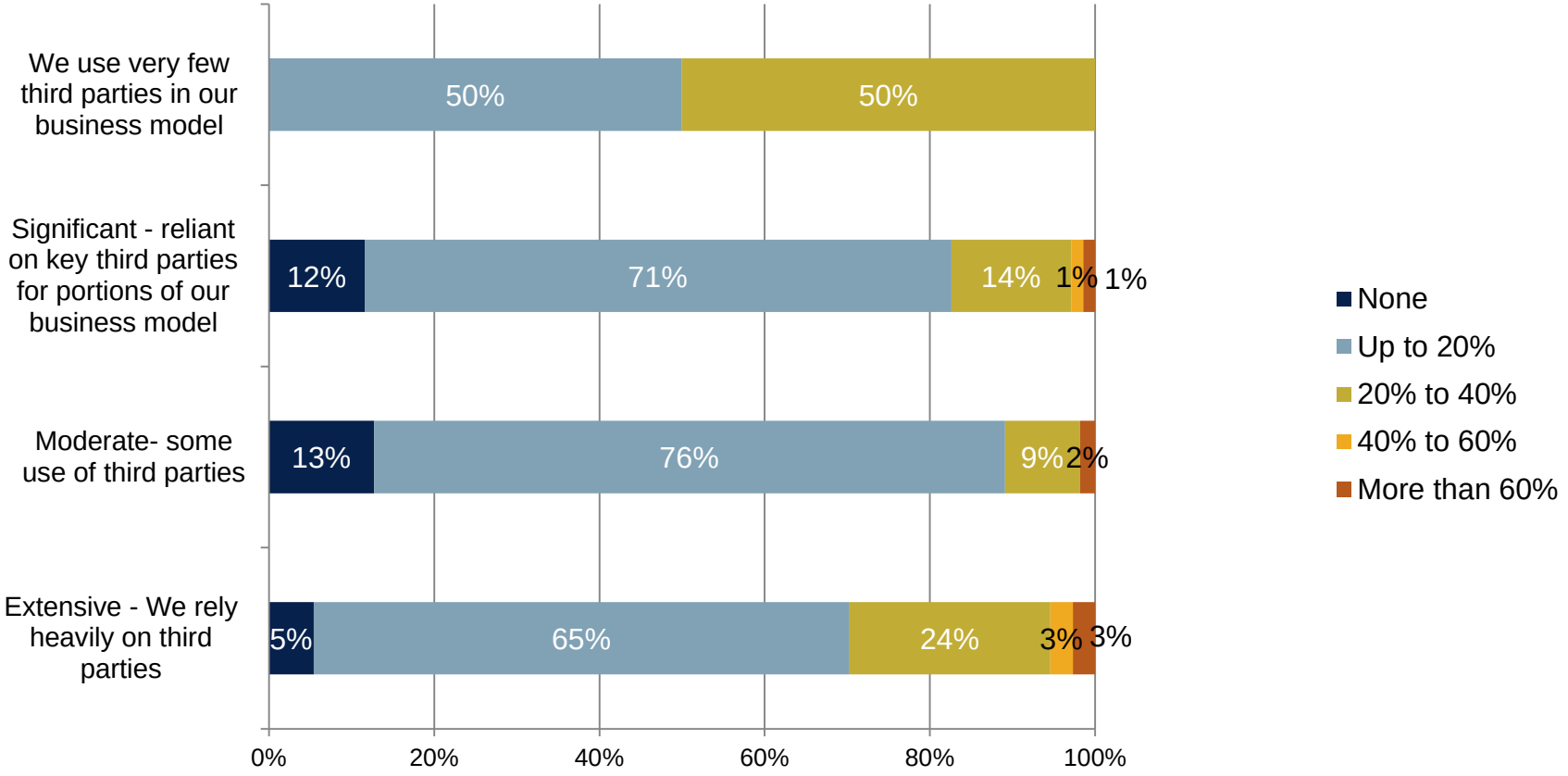
- What percentage of your company's total internal audit resources are expended on third-party risk matters?
  - A. <5%
  - B. 5% - 9%
  - C. 10% - 20%
  - D. 30% - 40%
  - E. Greater than 40%
  - F. Not sure

# The Role of Internal Audit in Third-Party Risk Management



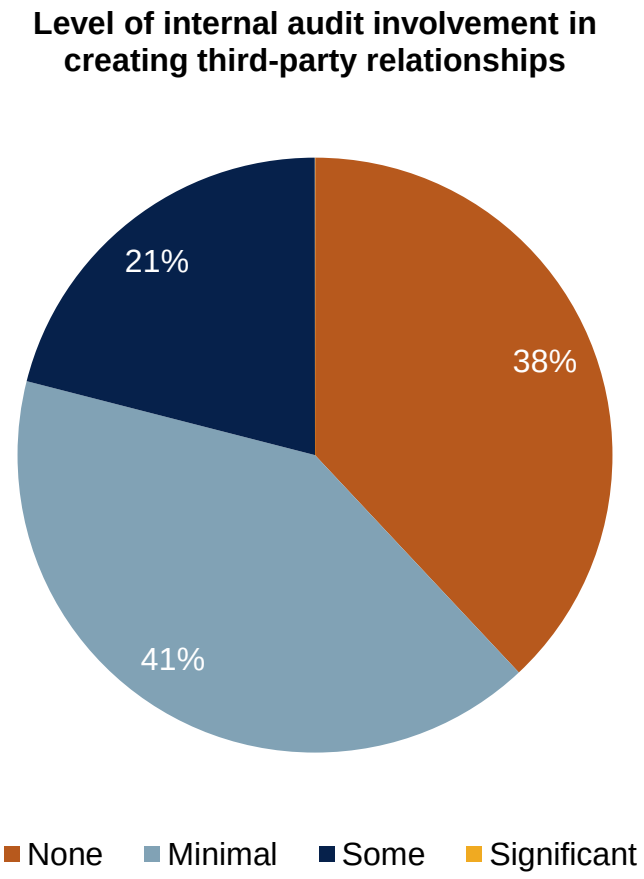

Source: "Closing the Gaps in Third-Party Risk Management, Defining a Larger Role for Internal Audit," December 2013, Sponsored by Crowe Horwath LLP

# Third-Party Use Compared to Internal Audit Resources Spent on Third-Party Risk




Source: "Closing the Gaps in Third-Party Risk Management, Defining a Larger Role for Internal Audit," December 2013, Sponsored by Crowe Horwath LLP

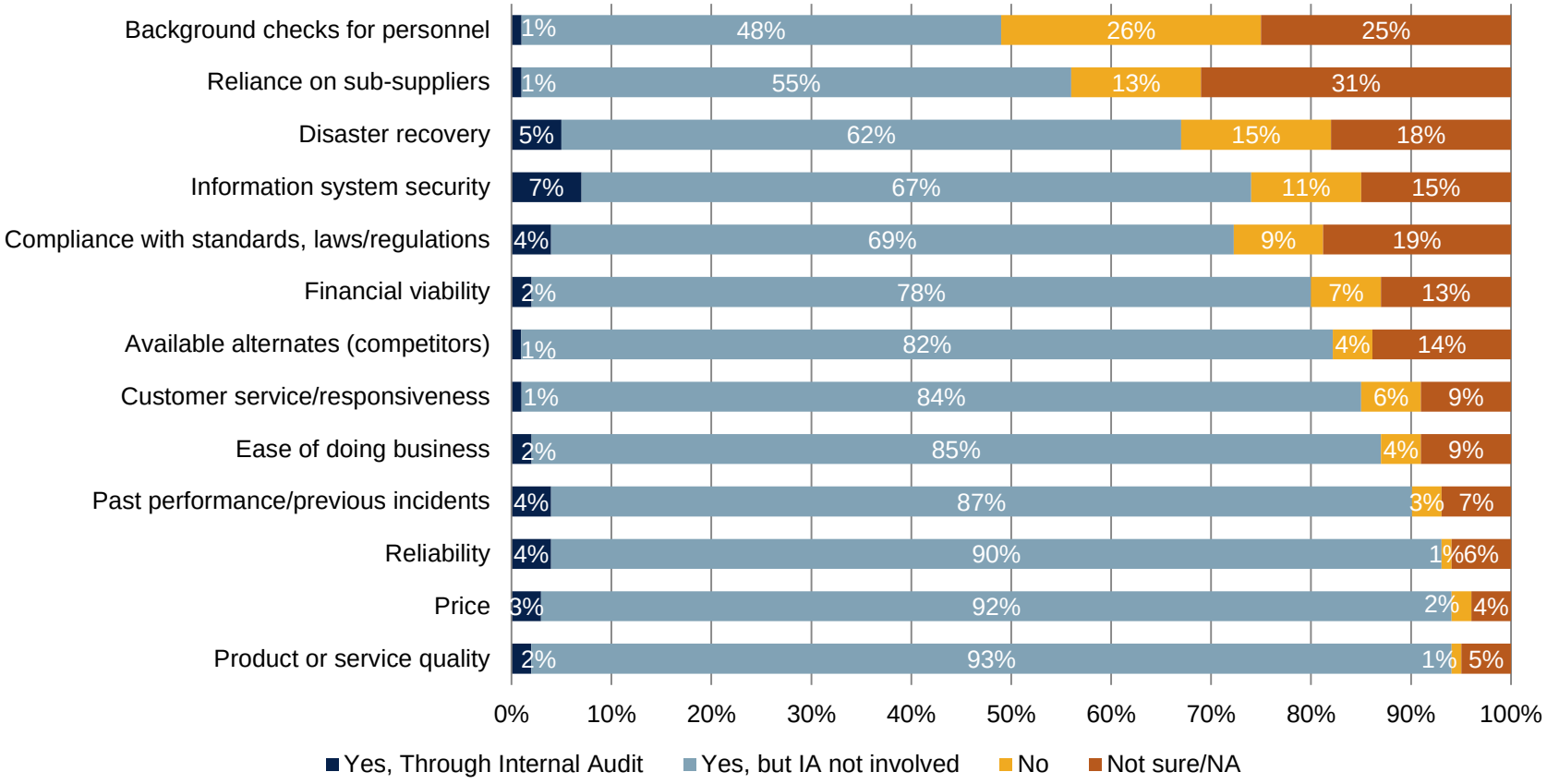
# Internal Audit's Involvement in the Third-Party Decisions




Source: "Closing the Gaps in Third-Party Risk Management, Defining a Larger Role for Internal Audit," December 2013, Sponsored by Crowe Horwath LLP

# The Role of Internal Audit in Third-Party Risk Management

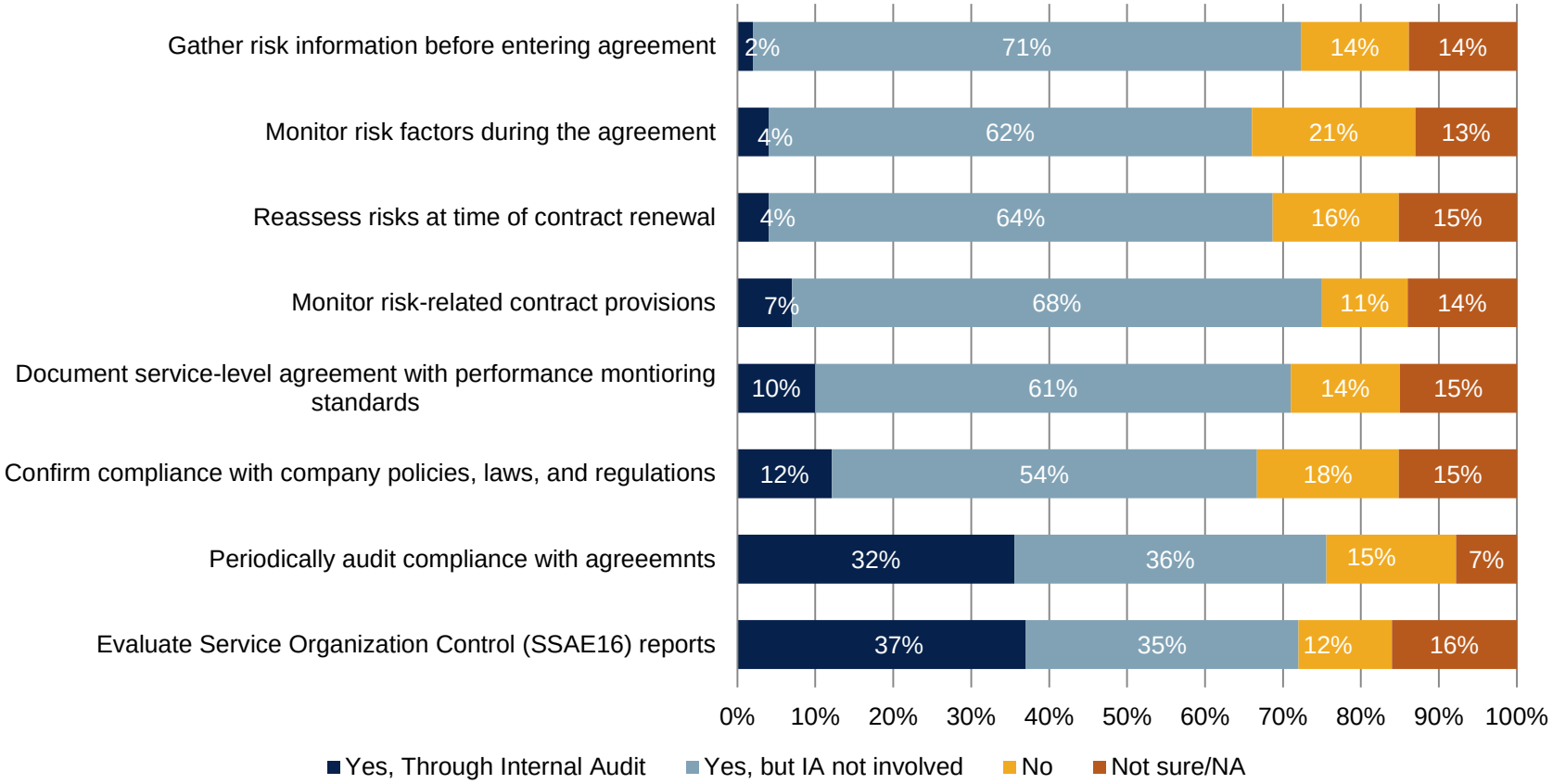
**When selecting or renewing a third party, what factors does your organization consider and how?**




Source: "Closing the Gaps in Third-Party Risk Management, Defining a Larger Role for Internal Audit," December 2013, Sponsored by Crowe Horwath LLP

# Monitoring Third Parties

**When selecting or renewing a third party, what factors does your organization consider and how?**

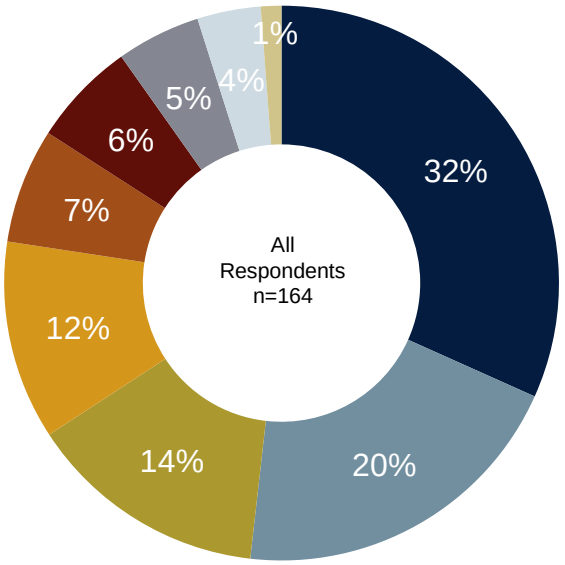



Source: "Closing the Gaps in Third-Party Risk Management, Defining a Larger Role for Internal Audit," December 2013, Sponsored by Crowe Horwath LLP

# Who Owns Third-Party Risk?

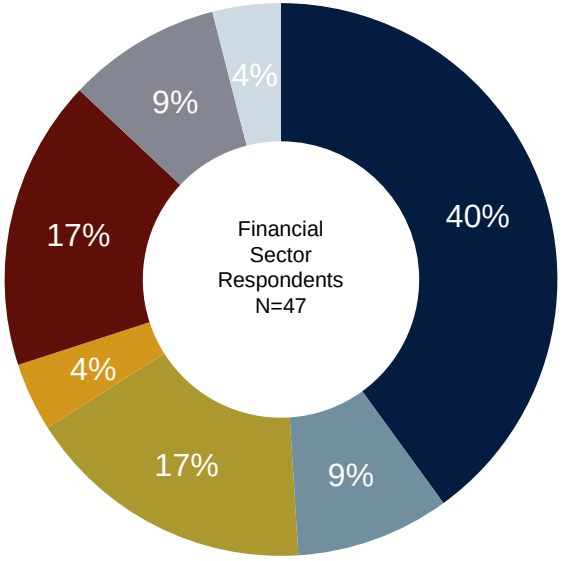
**Who has primary day-to-day responsibility for evaluating and overseeing third-party risk?**

**All Respondents**




- Business unit/functional leadership
- Individual BU or operational managers
- Decentralized risk management in BU
- Not clearly defined
- Procurement
- Centralized, enterprise-wide risk management
- Other
- Corporate leadership
- Don't know

**Financial Sector Respondents**




Source: "Closing the Gaps in Third-Party Risk Management, Defining a Larger Role for Internal Audit," December 2013, Sponsored by Crowe Horwath LLP

# Internal Audit's Role

## Consulting

- Assist management in identifying third-party risks (universe and ranking)
- Assist management in aggregating third-party risk management activities
- Assist management in linking the regulatory risks to the third-party program
- Identify process improvements in third-party interactions

## Assurance

- Assess the capabilities for managing third-party risks and how they align with the organization's ERM strategies
- Evaluate the adequacy of assurance activities performed by management
- Test third-party compliance with regulations or policies
- Evaluate management's risk identification, monitoring, and response activities
- Evaluate management's programs for supply chain resiliency

# Polling Question 3

- Which types of activities are your internal audit department most likely to be involved in, over the next two years, with respect to third-party risk management initiatives or audit activity?
  - A. Consulting services
  - B. Assurance services
  - C. Both
  - D. Neither or no expected internal audit involvement in third party risk

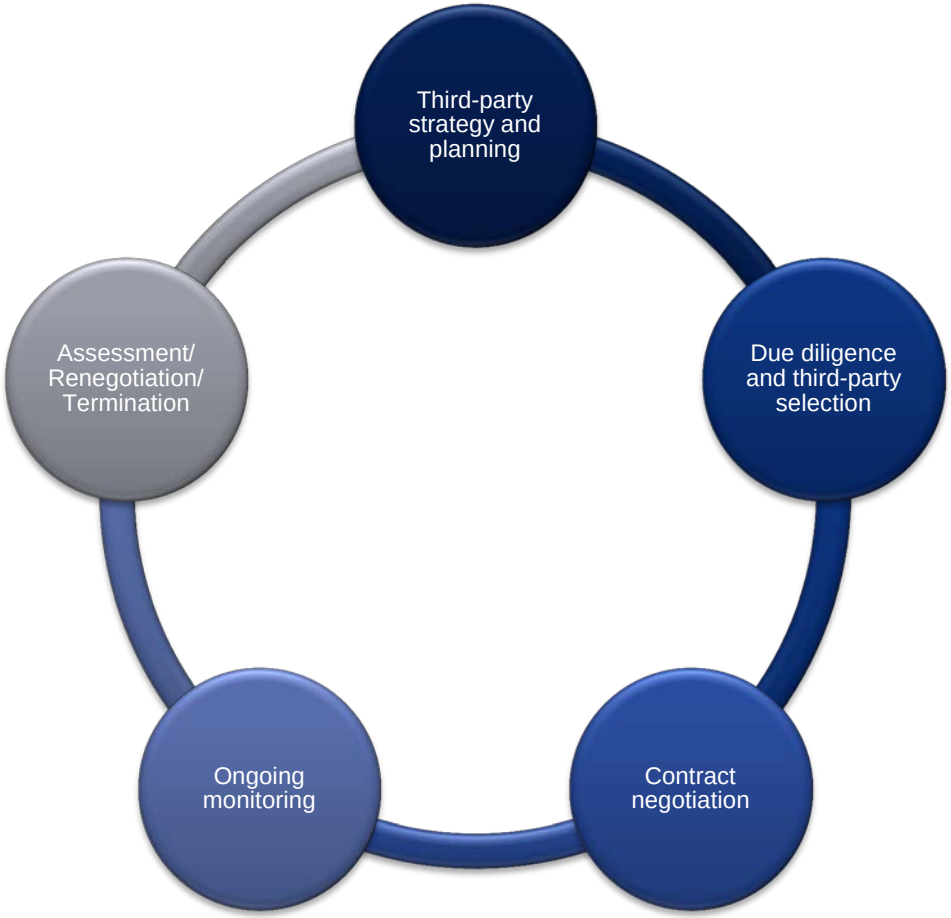
**Consulting**

- Assist management in identifying third party risks (universe and ranking)
- Assist management in aggregating third party risk management activities
- Assist management in linking the regulatory risks to the third party program
- Identify process improvements in third party interactions

**Assurance**

- Assess the capabilities for managing third party risks and how the align with the organizations ERM strategies
- Evaluate the adequacy of assurance activities performed by management
- Test third party compliance with regulations or policies
- Evaluate management's risk identification, monitoring and response activities
- Evaluate management's programs for supply chain resiliency

# Case Studies



# About Crowe's Third-Party Risk Services

- Thought leadership
  - Extensive research on industry trends
    - CFO Magazine | IIA Research Foundation | Compliance Week | National Association of Corporate Directors
    - Third-party risk management
    - Anti-corruption programs
    - Conflict minerals
    - Extensive webinars
  - Methods and Technology
    - Crowe® RAMP for Third Parties
    - Crowe Third Party Risk Management Framework
    - Conflict Minerals Compliance Tool

# Crowe Third-Party Risk Management Framework

- A framework to pull together and assist in coordination of all the risk management activities in a company's third-party risk program
- A platform or road map to assist management in improving third-party risk management efforts

# Third-Party Risk Management Capability Maturity Model

| Third-Party Risk Program Component | Initial | Repeatable | Defined | Managed | Optimizing |
|---|---|---|---|---|---|
| **Governance and Organization** | ▪ Minimal coordination<br>▪ Little to no governance or oversight<br>▪ Lacking standards and methods | ▪ Limited senior management commitment to standard practices related to third parties<br>▪ Organizational awareness that controls are needed around third-party risk | ▪ Policies are established<br>▪ There is a formal organization for managing the risks of third parties (committee, central group, executive leader, etc.)<br>▪ Defined escalation processes<br>▪ Meaningful board involvement for high risk areas | ▪ Risk management activities are embedded in operational processes<br>▪ Third party risk is quantitatively managed across business functions<br>▪ Monitoring is performed at the business unit and enterprise level | ▪ Third parties are continually evaluated through the organization<br>▪ Resources allocated as needed to address third-party objectives or emerging risks<br>▪ High-level of cross functional coordination in monitoring risks |
| **Risk Identification and Assessment** | ▪ Activities are not linked to the organization's ERM framework<br>▪ Differing tolerances and risk assessment levels<br>▪ Limited perspective of risk levels across the organization | ▪ Specific activities are in place to assess risk, although they may differ across the organization | ▪ Periodic reporting and oversight of risk management activities<br>▪ Formal methods for aggregating and monitoring risk profiles of third parties are in place<br>▪ There is a common approach at the enterprise level with consistent risk ratings<br>▪ Processes for managing third-party risks are incorporated in standard business processes | ▪ Internal benchmarking/ metrics are available to evaluate and monitor key third parties and related risk areas | • Advanced indicators of red flags<br>• Benchmarking with peers as needed<br>• Calculated risk taking or reduction activities<br>• Risk factors embedded into decision making on overall third party relationship |
| **Assurance Activities** | ▪ Little or no assurance on third party risk matters<br>▪ Those assurance activities that are in place<br>▪ Differing assurance approaches across the organization | ▪ Prescribed assurance activities are in place for key third parties, although the approach may not be consistent | ▪ Formal enterprise approach to identifying and assessing third parties, based on risk | ▪ Trends are monitored and improvements addressed across the third-party portfolio<br>▪ Periodic assurance activities tied to risk levels and tolerances | • Real-time monitoring or automation of compliance activities<br>• Assurance and ultimately reliance on the third party's own risk management activities |

Source: "Closing the Gaps in Third-Party Risk Management, Defining a Larger Role for Internal Audit," December 2013, Sponsored by Crowe Horwath LLP | The Capability Maturity Model was developed by Carnegie Mellon University to define the level of maturity in a process.

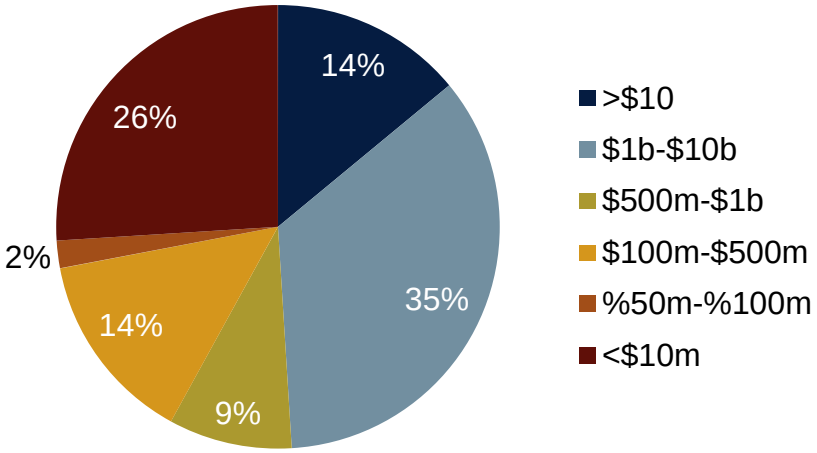
# Polling Question 4

- Where is your company today in terms of third-party risk management maturity?
  - A. Initial
  - B. Repeatable
  - C. Defined
  - D. Managed
  - E. Optimizing

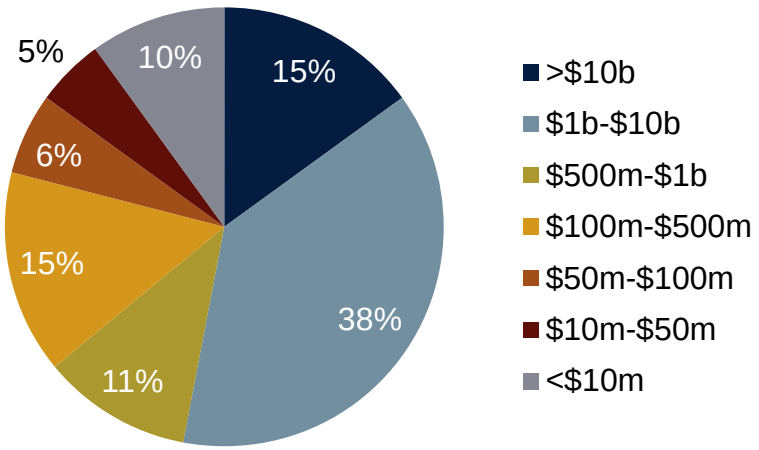
| Third Party Risk Program Component | Initial | Repeatable | Defined | Managed | Optimizing |
|---|---|---|---|---|---|
| **Governance and Organization** | ▪ Minimal coordination<br>▪ Little to no governance or oversight<br>▪ Lacking standards and methods | ▪ Limited senior management commitment to standard practices related to third parties<br>▪ Organizational awareness that controls are needed around third party risk | ▪ Policies are established<br>▪ There is a formal organization for managing the risks of third parties (committee, central group, executive leader, etc.)<br>▪ Defined escalation processes<br>▪ Meaningful board involvement for high risk areas | ▪ Risk management activities are embedded in operational processes<br>▪ Third party risk is quantitatively managed across business functions<br>▪ Monitoring is performed at the business unit and enterprise level | ▪ Third parties are continually evaluated through the organization<br>▪ Resources allocated as needed to address third party objectives or emerging risks<br>▪ High level of cross functional coordination in monitoring risks |
| **Risk Identification and Assessment** | ▪ Activities are not linked to the organization's ERM framework<br>▪ Differing tolerances and risk assessment levels<br>▪ Limited perspective of risk levels across the organization | ▪ Specific activities are in place to assess risk, although they may differ across the organization | ▪ Periodic reporting and oversight of risk management activities<br>▪ Formal methods for aggregating and monitoring risk profiles of third parties are in place<br>▪ There is a common approach at the enterprise level with consistent risk ratings<br>▪ Processes for managing third party risks are incorporated in standard business processes | ▪ Internal benchmarking/ metrics are available to evaluate and monitor key third parties and related risk areas | • Advanced indicators of red flags<br>• Benchmarking with peers as needed<br>• Calculated risk taking or reduction activities<br>• Risk factors embedded into decision making on overall third party relationship |
| **Assurance Activities** | ▪ Little or no assurance on third party risk matters<br>▪ Those assurance activities that are in place<br>▪ Differing assurance approaches across the organization | ▪ Prescribed assurance activities are in place for key third parties, although the approach may not be consistent | ▪ Formal enterprise approach to identifying and assessing third parties, based on risk | ▪ Trends are monitored and improvements addressed across the third party portfolio<br>▪ Periodic assurance activities tied to risk levels and tolerances | • Real time monitoring or automation of compliance activities<br>• Assurance and ultimately reliance on the third party's own risk management activities |

# Respondents by Size

**Survey Respondents' Annual Revenue (Non-Financial Services) (USD)**

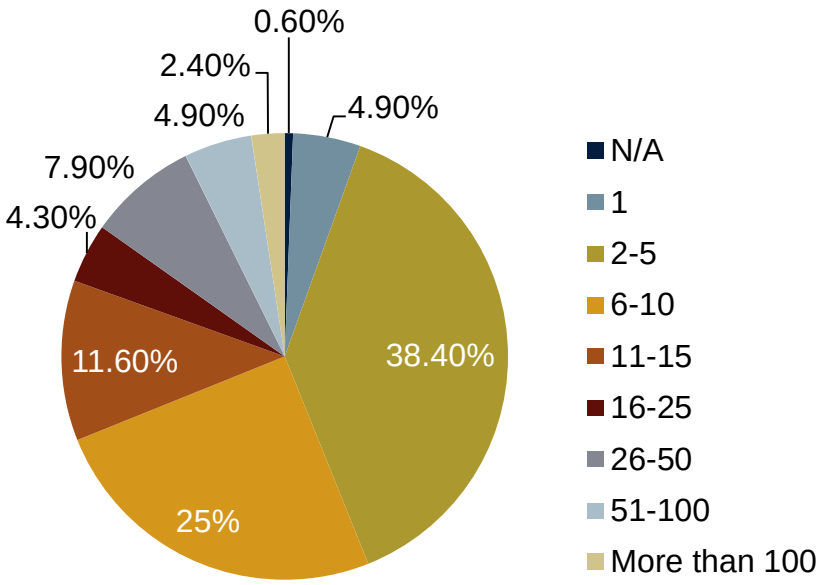



**Survey Respondents' Total Assets (Financial Services) (USD)**




Source: "Closing the Gaps in Third-Party Risk Management, Defining a Larger Role for Internal Audit," December 2013, Sponsored by Crowe Horwath LLP

# Respondents by Internal Audit Department Size




Source: "Closing the Gaps in Third-Party Risk Management, Defining a Larger Role for Internal Audit," December 2013, Sponsored by Crowe Horwath LLP

# Questions?

# For more information, contact:

Rick Warren
Direct 404.442.1606
rick.warren@crowehorwath.com

To obtain your copy of the IIARF Research Report:
www.crowehorwath.com/iiareport