Risk Management Strategies that Deliver Business Performance

French Caldwell

Vice President and
Gartner Fellow
Twitter: @iTGuru

USS San Francisco

Source: U.S. Navy

…. The New 'ab'Normal

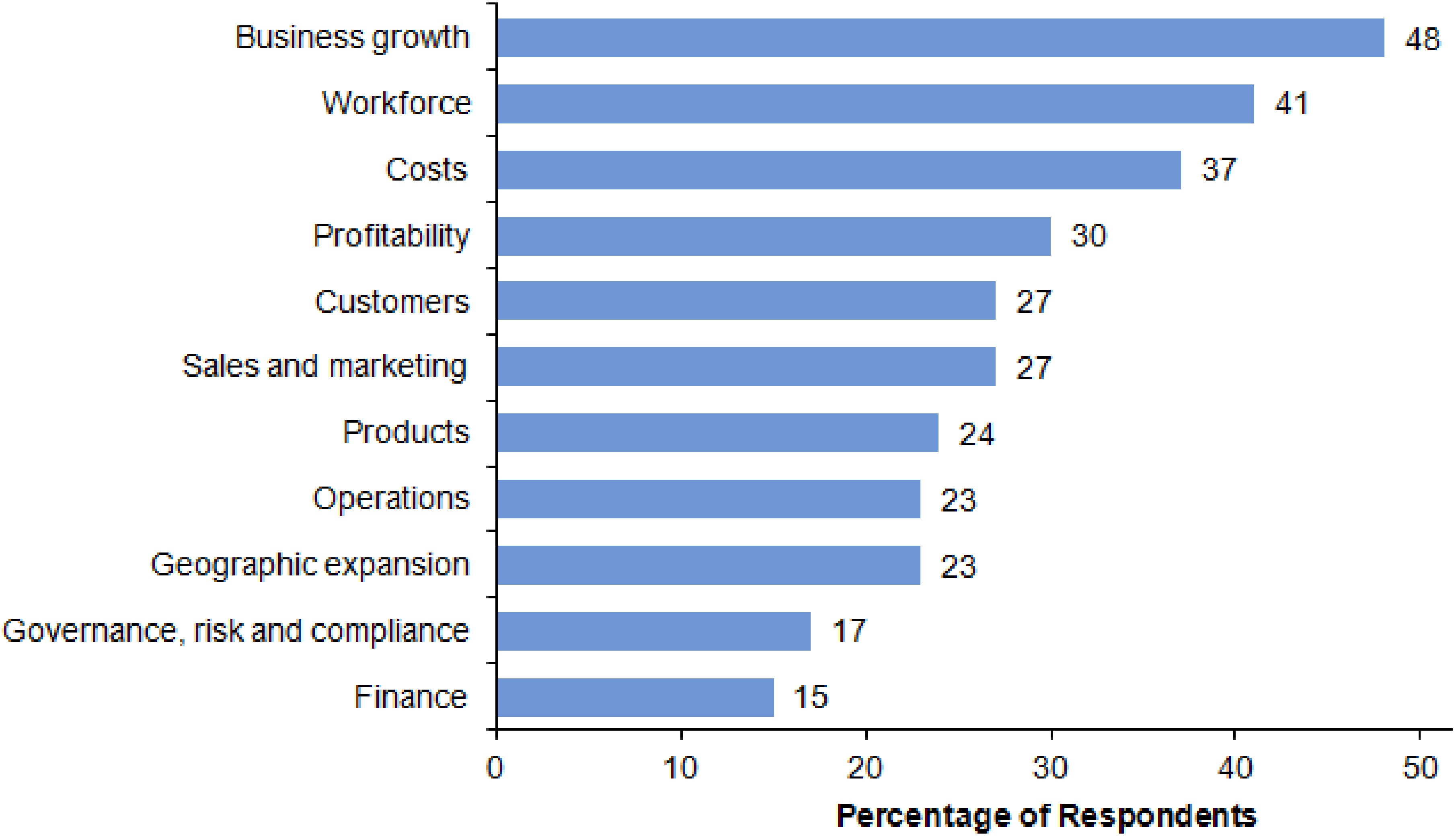
Regulatory Failures

Erosion of Trust

Demands for Accountability

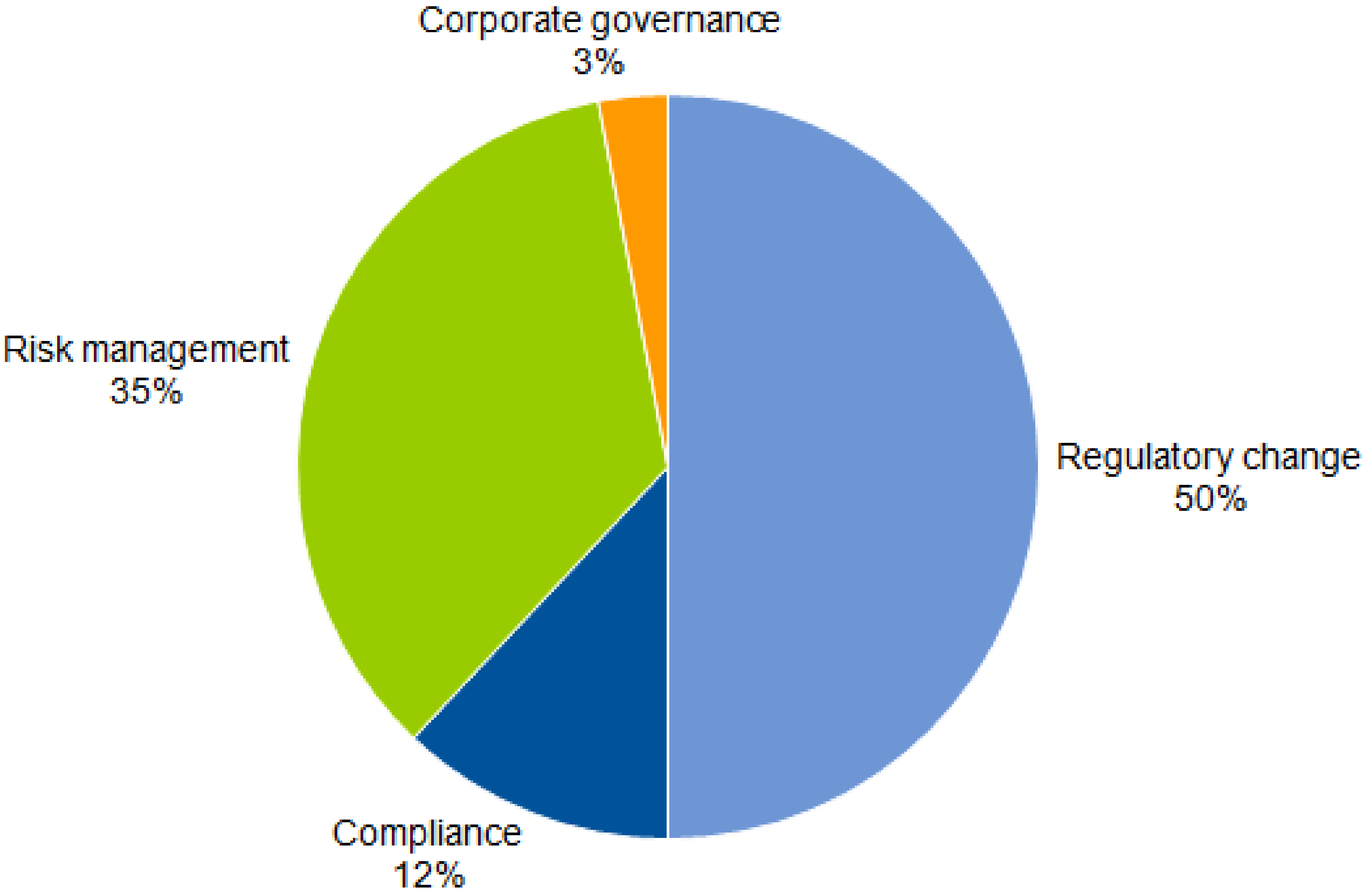
IT Led Political Change

Global CEO and Senior Executive Survey – Top Business Priorities for 2013

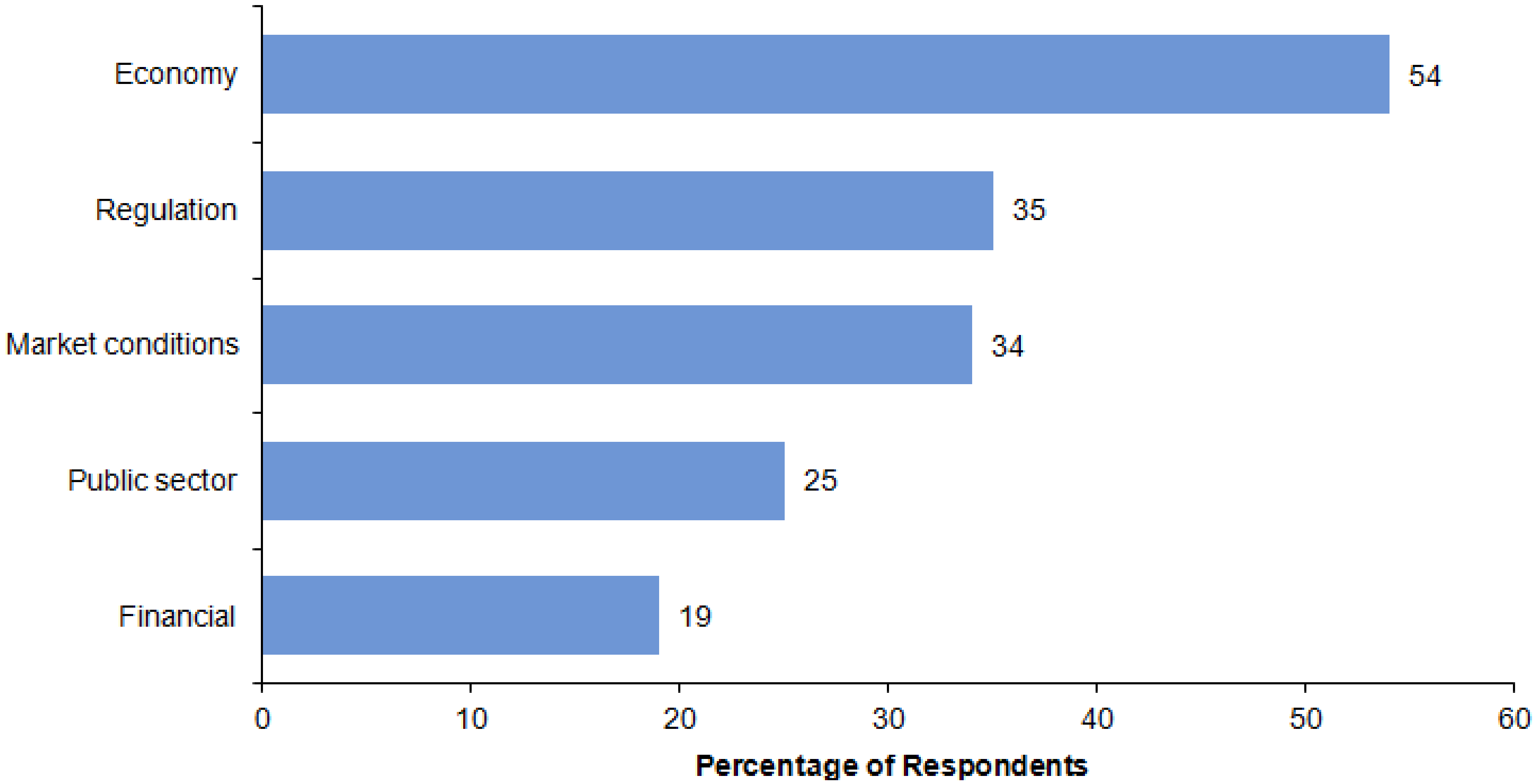


Gartner.

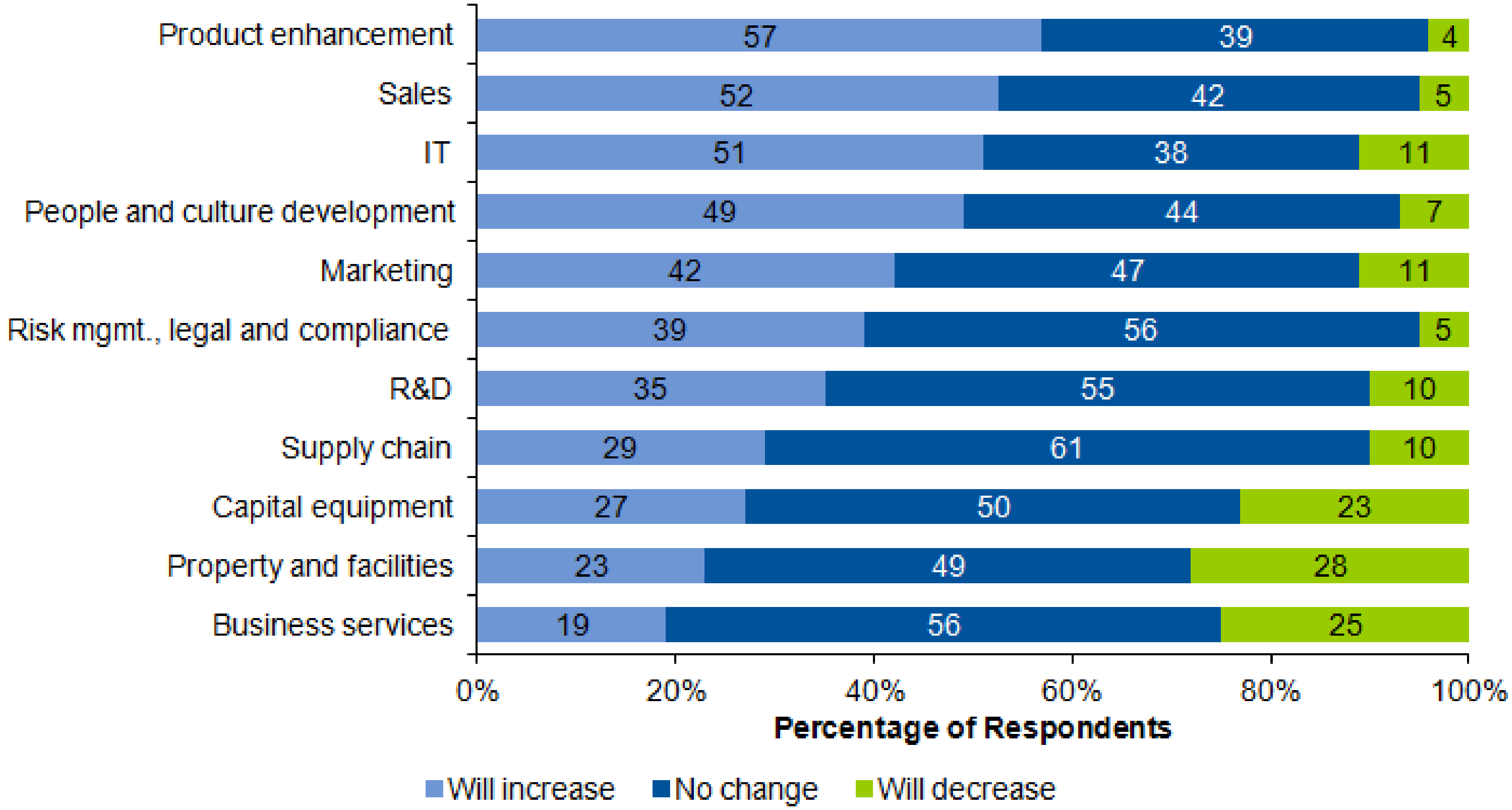
Global CEO and Business Executives Survey: Breakdown of GRC Business Priorities



Global CEO and Senior Executive Survey – Top Business Risks for 2013



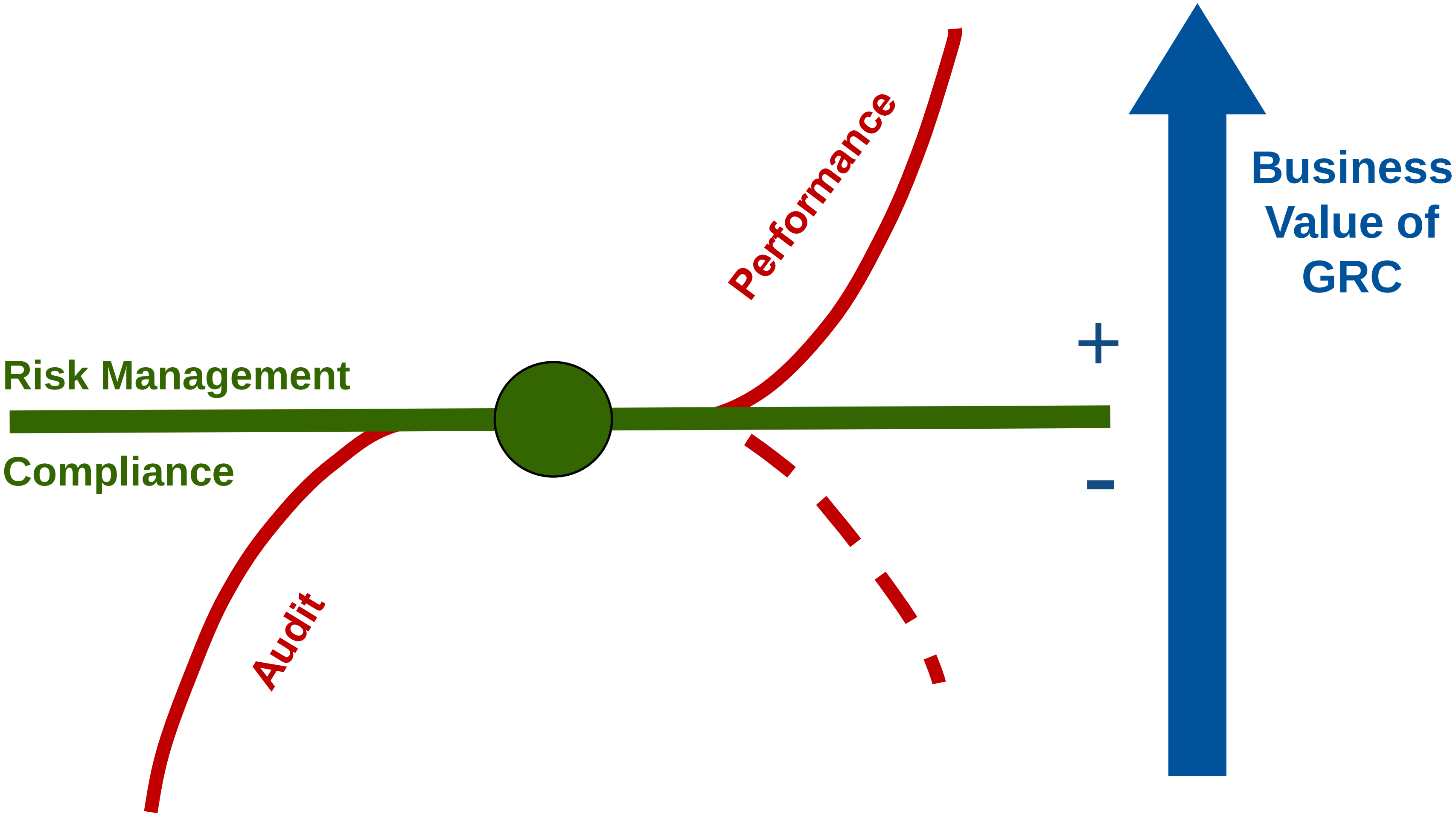
Global CEO and Senior Executive Survey – Investment Priorities for 2013



Gartner

GRC Is Wasteland

Inflection Point of Business Value



Gartner

Two Great Tastes That Taste Great Together

ERM

"a holistic treatment of all strategic, operational, financial reporting, and legal and compliance risks, including the IT and information management components of those risks"

GRC

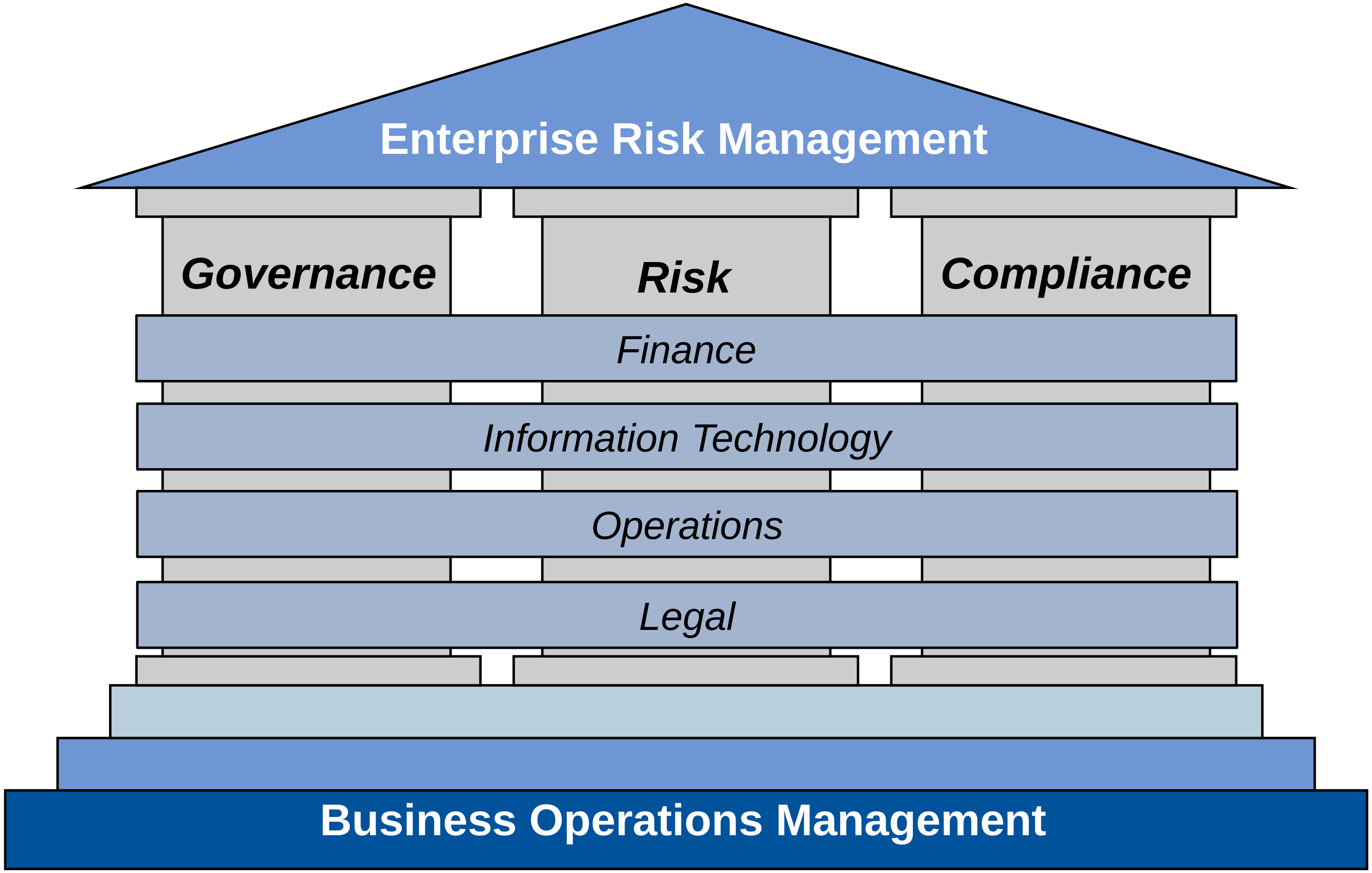
“an integrated set of processes and enabling technologies that supports a company's ability to increase risk awareness and accountability, and improve business decision making”

Key Words

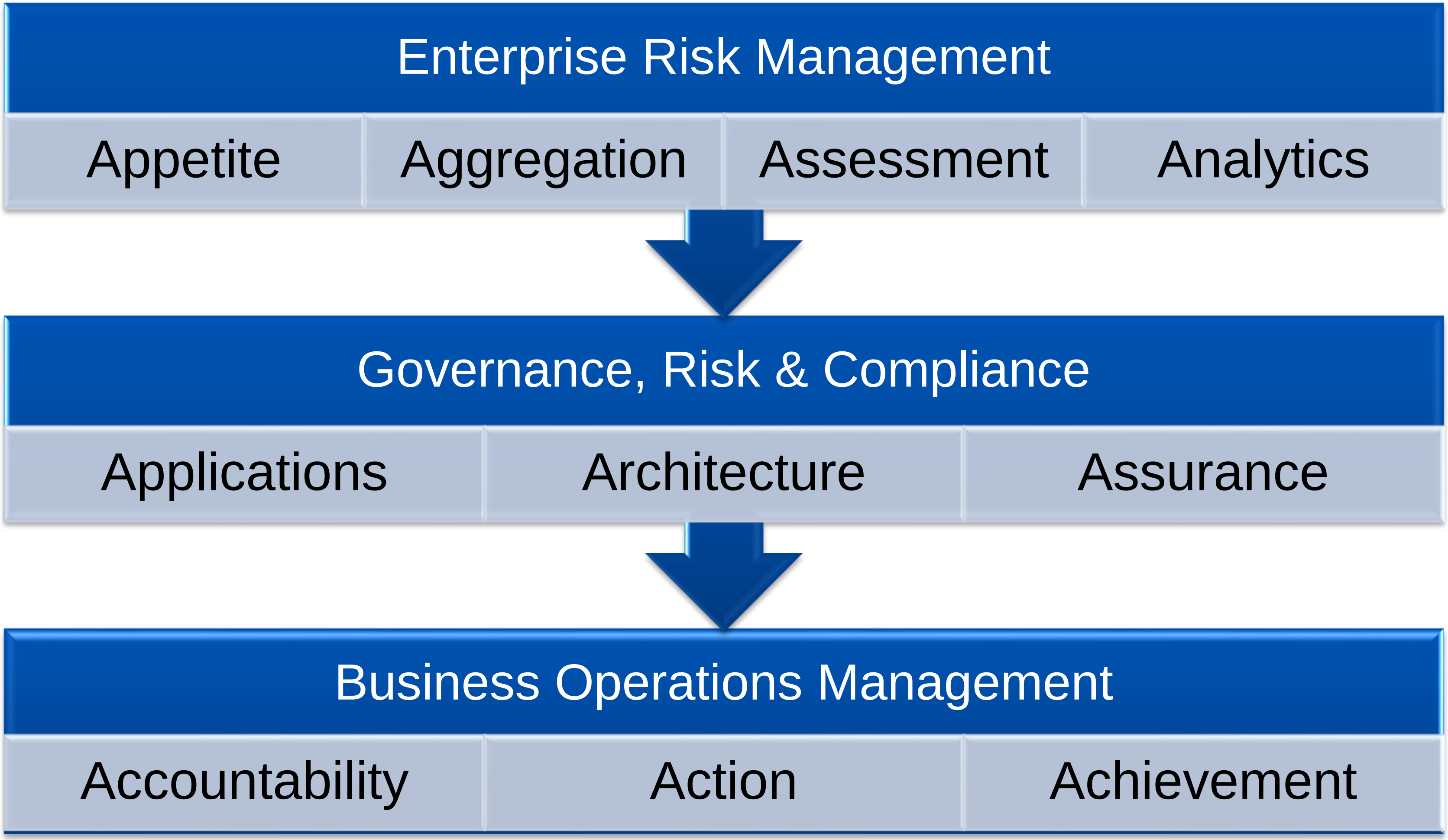
holistic, strategic, operational, financial reporting, legal/compliance, IT

integrated, processes, technologies, awareness, accountability, business, decision-making

ERM / GRC Blueprint



10 A’s of Successful Risk Management & Compliance



Enterprise Risk Management

Appetite | Aggregation | Assessment | Analytics

Governance, Risk & Compliance

Applications | Architecture | Assurance

Business Operations Management

Accountability | Action | Achievement

Key Questions to Answer - ERM

Appetite

- How much risk are we willing to accept to achieve our strategic goals?

Aggregation

- How do we view our risks in relation to our strategic goals?
- How do we understand and articulate our total risk exposure in relation to a given strategic objective?

Key Questions to Answer - ERM

Assessment

- What is our current level of inherent and residual risk related to our strategic goals?
- How are residual risks and control effectiveness monitored?
- How is the need for and effectiveness of remediation determined and assessed?

Analytics

- How do our key risk indicators impact our key performance indicators?
- How can we model risk events that will have a material impact our business operations?
- What risk tolerance limits are required to maintain our stated risk appetite?

Key Questions to Answer - GRC

Applications

- What technology is required to enable collaboration and communication of risk and compliance related information to support business performance and decision making?
- What technology enables automation of risk management and compliance processes and reporting?
- What technology enables automation of controls and risk monitoring?

Architecture

- Are risk management and compliance projects and initiatives aligned with governance objectives?
- How are GRC applications, automated and manual controls, risk monitoring, and risk and compliance reporting incorporated into enterprise architecture?
- How does the GRC program contribute to targeted business outcomes?

Key Questions to Answer - GRC

Assurance

- What policies, processes and controls are required to meet strategic objectives as well as legal and regulatory mandates?
- How do we know that the risk management and compliance program is effective, and remains aligned to business objectives?
- Are the risk controls functioning consistently over time?
- Do these controls need to be revised or redesigned based on a changing risk landscape?

Key Questions to Answer – Business Ops

Accountability

- How do we reinforce the ownership of risk and control within the enterprise?

Action

- How can we ensure that employees act in the best interests of the company and within established risk tolerances?

Achievement

- What risk metrics are required and how are they linked to performance metrics to ensure the desired business outcome?

Recommendations

- ✓ Develop an ERM framework that focuses on risk ***appetite***, risk ***aggregation***, risk ***assessment*** and risk ***analytics***.
- ✓ Implement a GRC infrastructure that includes the right technology ***applications***, the necessary ***architecture*** and the appropriate level of ***assurance***.
- ✓ Promote risk ***accountability*** that drives the right ***actions*** that lead to the ***achievement*** of desired business outcomes.

Action Plan for Risk Managers

Monday Morning

- *Evaluate current Risk Management & Compliance Program against the ERM / GRC Blueprint*.
- *Develop list of key stakeholders and program areas to include in integration effort*.

Next 90 Days

- *Identify gaps and/or integration opportunities using the 10 A's*.
- *Engage board members, senior management and business operations management to answer key questions*.

Next 12 Months

- *Define ERM framework and GRC infrastructure build requirements*.
- *Begin ERM / GRC integration effort*.