



Enterprise Risk Management: Moving from Compliance-based auditing to a Risk-based approach

Lisa Young
Managing Director, Dyntek Services
813-571-9008
Lisa.Young@dyntek.com





Agenda

- Internal Audit Paradigms
- Risk
- Risk Management
- Frameworks for Risk Assessment
- Conducting a Risk Assessment
- Moving to Enterprise Risk Management

What is a paradigm?

- Set of rules for looking at the world
- Like a comfortable shoe





Internal Audit Paradigms

- Phase 1 – since we could count
 - Focus on observation and counting
- Phase 2 – since early 1940's
 - Focus on controls
- Phase 3 – since late 1990's
 - Focus on business process and risk



Definition of Internal Control

A process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives.



Categories of Internal Control

- Effectiveness & efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations



Components of Internal Control

1. Control Environment
2. Risk Assessment
3. Control Activities
4. Information and Communication
5. Monitoring

Internal Audit Focus

- Old paradigm (Controls)
 - Internal controls
- New paradigm (ERM)
 - Business risks



Internal Audit Tests

- Old paradigm (Controls)
 - Important controls
- New paradigm (ERM)
 - Significant risks

Internal Audit Methods

- Old paradigm (Controls)
 - Detailed control testing
- New paradigm (ERM)
 - Looking at the risks to the whole business



Internal Audit Recommendations

- Old paradigm (Controls)
 - Internal controls strengthened
 - Cost/Benefit analysis
 - Efficient and effective



Internal Audit Recommendations

- New paradigm (ERM)
 - Risk Management
 - Avoid/Diversify Risk
 - Share/Transfer Risk
 - Control/Accept Risk



Internal Audit Reports

- Old paradigm (Controls)
 - Address functional controls
- New paradigm (ERM)
 - Address the business process risks

Internal Audit Role

- Old paradigm (Controls)
 - Independent assessment
- New paradigm (ERM)
 - Integral to Risk Management and Corporate Governance

Old Audit Paradigm

- Set of yearly financial statements accompanied by annual audit report



New Audit Paradigm

- Set of real-time financial and non-financial information
- Accompanied by continuous assurance to clients and the public





What is driving the paradigm shift?

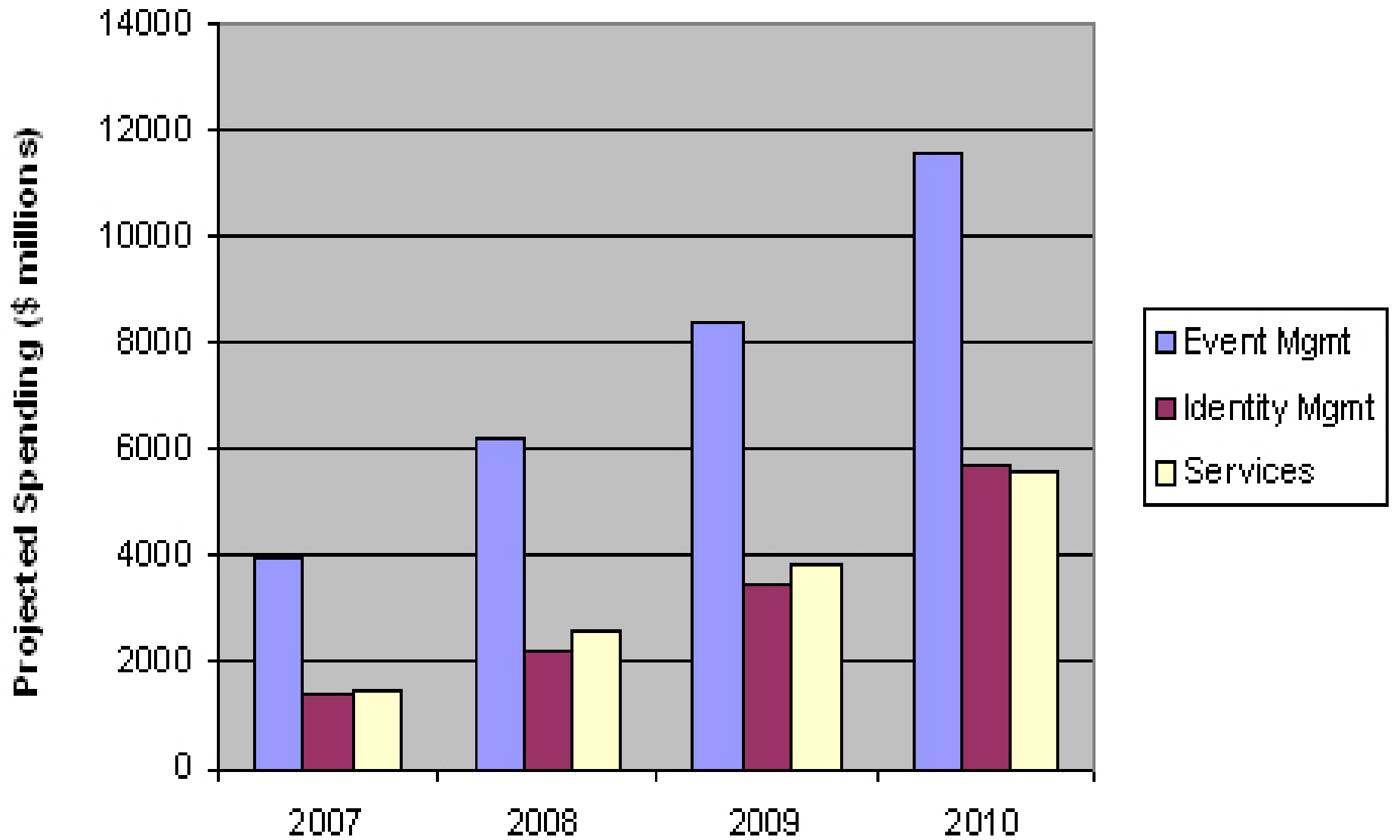
- Financial and Cultural realities
 - Corporate disasters
 - Customer data privacy
- Global spotlight on Corporate Governance
- Regulatory Actions & Industry initiatives
 - SEC, SOX, Basel II, COSO, Turnbull
- Realizing value from compliance efforts



Corporate Governance

- IT is a significant component of the systems of internal control
- Business controls over the use and application of IT cannot logically be separated from the other elements of the control environment.
- Converging of all forms of Security

Major Trends in Convergence Spending





Risk





What is Risk?

The possibility of direct or indirect loss due to a failure of people, process or systems, or due to external events.

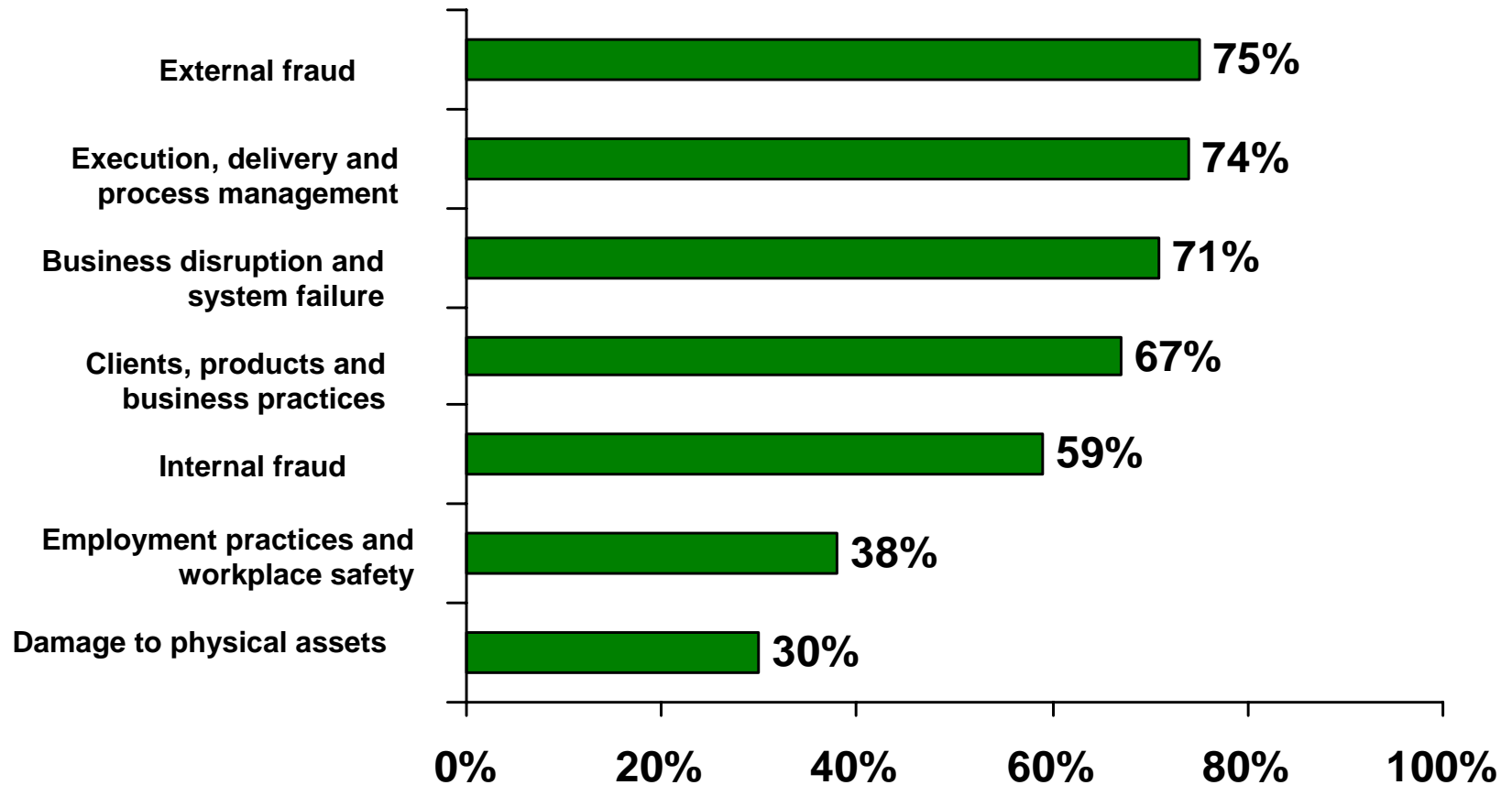


Types of Risk

- Compliance Risk
- Legal Risk
- Reputation Risk
- Business Risk
- Operational Risk
- Any of these risks can result in increased write-offs, additional expenses , loss of revenue, failure to meet service delivery goals.....



Sources of Operational Risk





Risk Management





What is Risk Management?

The total process to identify, control, and manage the impact of uncertain harmful events, commensurate with the value of the protected assets.



More simply put...

Determine what your threats are and then decide on a course of action to deal with those risks.



Even more colloquially...

- What's your threshold for pain?
- Risk Appetite?
- Do you want failure to deal with this risk to end up on the front page of the *Wall Street Journal*?



Traditionally, risks were managed within organizational “silos”

	Strategic Risk	Business Risk	Financial Risk	Operational Risk
Who	<ul style="list-style-type: none">• Board of Directors• CEO	<ul style="list-style-type: none">• Business Managers• Project Managers	<ul style="list-style-type: none">• CFO• Treasurer	<ul style="list-style-type: none">• Internal Audit• Compliance• IT
How	<ul style="list-style-type: none">• Strategic planning• EVA• Balanced scorecard	<ul style="list-style-type: none">• Product plans• Business reviews• Project management	<ul style="list-style-type: none">• Country and credit limits• Trading and ALM Limits• Financial derivatives	<ul style="list-style-type: none">• Controls• Audits• Contingency planning• Insurance

Risk Management

- **Goal - Protect the organization and the ability to perform its mission.**
- **Focus is *Mission*, not individual controls.**
- **Risk management is an essential management function of the business.**



Current Organizational view of Risk Management

- **Level I organizations see little value in proactive risk management.**
- **In Level II organizations, there is general awareness about risk management and some conceptual appreciation for its value in assuring that not all uncertainties become problems.**
- **Level III organizations are aware of risk management and they have set up some mechanisms to monitor risks.**
- **In Level IV, a broader risk management position is created to review “hot” spots, assist in risk assessment within the business units, and keep score.**
- **Level V organization, the CEO believes that risk management should be imbedded in every part of the organization. Business units track their progress against action plans. Training programs are in place. Internal audit evaluates the program to assure that the process is in place and working effectively.**



Frameworks for Risk Assessment





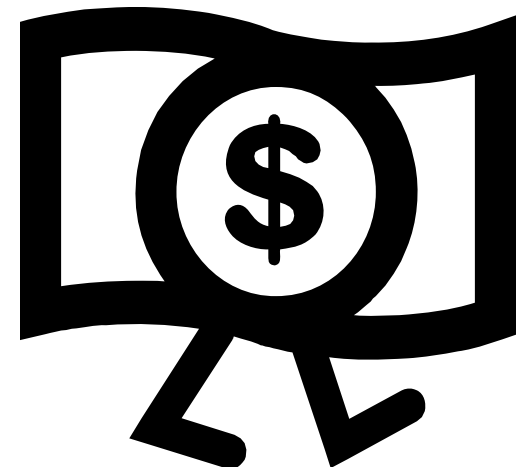
Common Frameworks

- COSO
- COBIT
- OCTAVE
- NIST



OCTAVE

- OCTAVE was developed by the Software Engineering Institute and CERT of Carnegie Mellon University
- Originally developed for Department of Defense for HIPAA compliance
- Your tax dollars at work





What Is OCTAVE?

- OCTAVE is a risk-based strategic assessment and planning technique for securing critical business assets
- It leverages people's knowledge of their organization's security-related practices and business processes.
- Threats to the most critical assets are prioritized to set the protection strategy for the organization



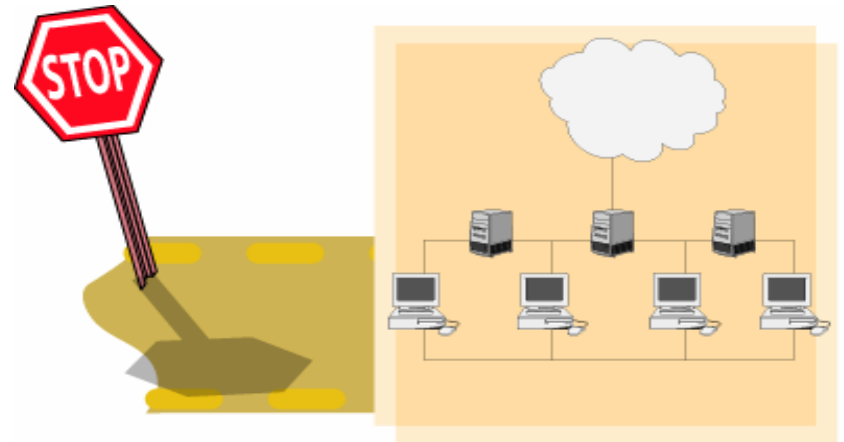


Organizational Gap



Enterprise Management

Business
Planning
Budget



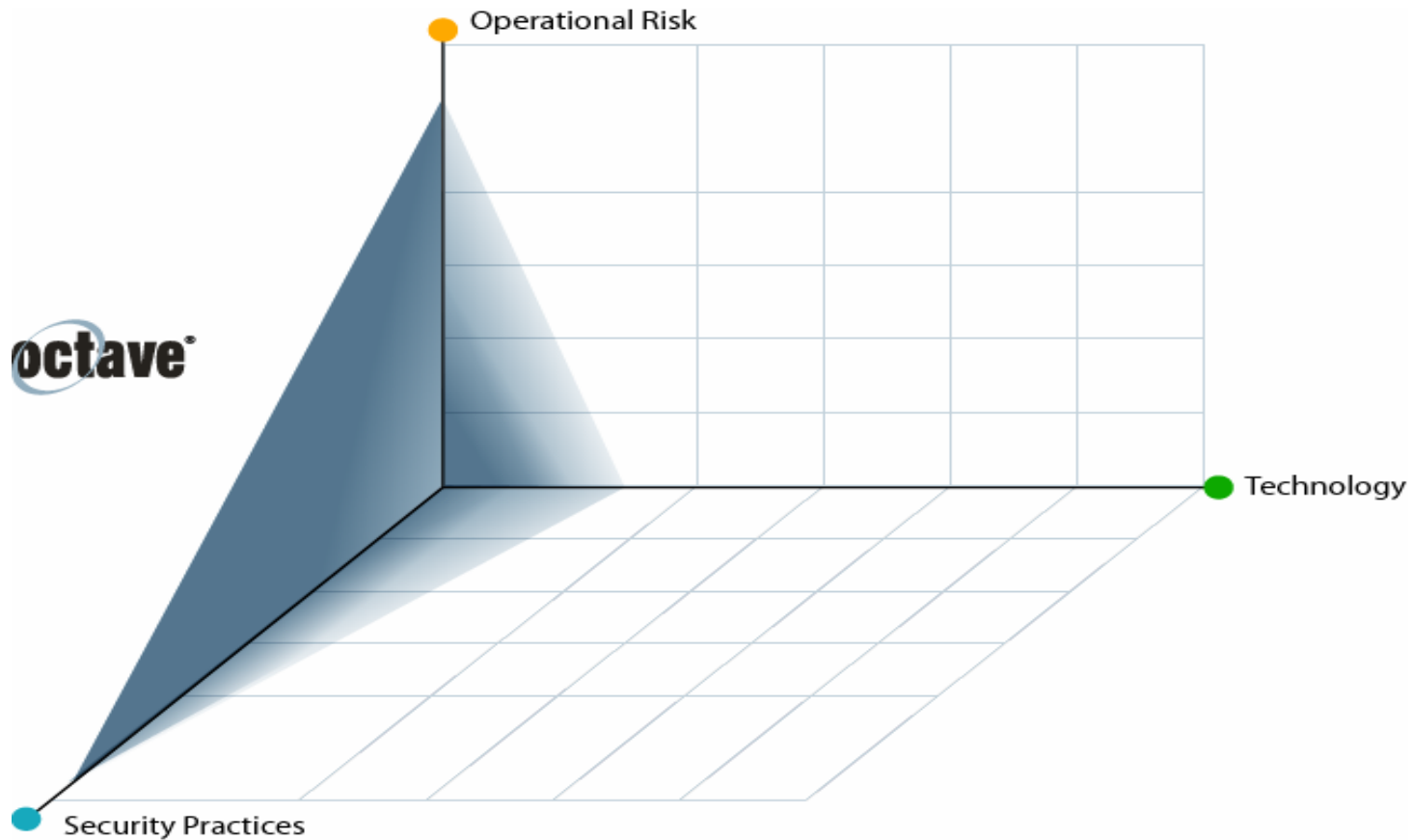
Network

Hack Points
Communication
Systems Administration
Network Support





A Practice-Based Approach



Outputs of OCTAVE

Protection Strategy



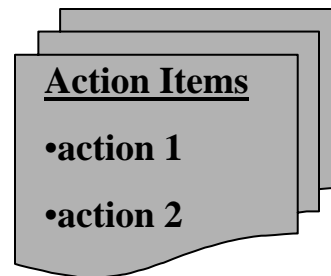
Whole Organization – Long Term

Risk Mitigation Plan



Protection for Critical Assets

Action List



Near-Term Actions – 30/60/90 days



Conducting a Risk Assessment





Facilitating the Discussion

- Inviting key players to a brainstorming session to identify and rank the greatest business risks company-wide.
- Conducting a risk assessment exercise with senior management and the board, either through interview, questionnaires, or a combination of the two, to pinpoint the most critical risks.
- Taking a look at the annual strategic plan to identify the key strategic risks to the organization.
- Staying on top of the changing risk profile of the organization by holding quarterly meetings with those responsible for developing the strategic plan.
- Grouping risks together based on how they relate to one another. Within each group, for example, the impact of certain risks may grow or diminish as other risks rise or fall. Or, as one risk is transferred or shared, another risk may emerge. This awareness of impacts and interdependencies offers increased understanding of which risks are critical and require more attention.



IIA Standards

- Require internal auditors to monitor and evaluate the effectiveness of an organization's risk management system
- Suggest the chief audit executive obtain an understanding of management and board expectations of the internal audit activity in the organization's risk management process. This understanding should be codified in the charters of the internal audit activity and audit committee.



IIA Recommendations

- If an organization has not established a risk management process, the internal auditor should bring this to management's attention along with suggestions for establishing such a process.



Typical RA Engagement

- Three to eight weeks
- Interviews with Senior Management, Operational Managers, Users and IT Staff
- Security Awareness surveys given
- Policy & procedure Gap analysis
- Physical security assessment
- Network Vulnerability assessment
- Remediation recommendation report
- \$10K to \$100K depending on scope



Benefits for Your Organization

- Identify risks that could prevent the business from achieving its mission.
- Learn to manage information security & risk outside of just technology.
- Create a protection strategy designed to reduce your highest priority risks.
- Position your site for compliance with data security requirements or regulations.



Operational Risk Management & Shareholder Value

- Identifies and prioritizes process improvement and de-risking opportunities for critical assets
- Improves management effectiveness by enhancing overall governance structure
- Enables more effective capital usage by introducing processes to assess exposure & integrate this with an economic capital model
- Enhances organizational capabilities & subsequent competitive positioning through continuous improvement



Moving to Enterprise Risk Management



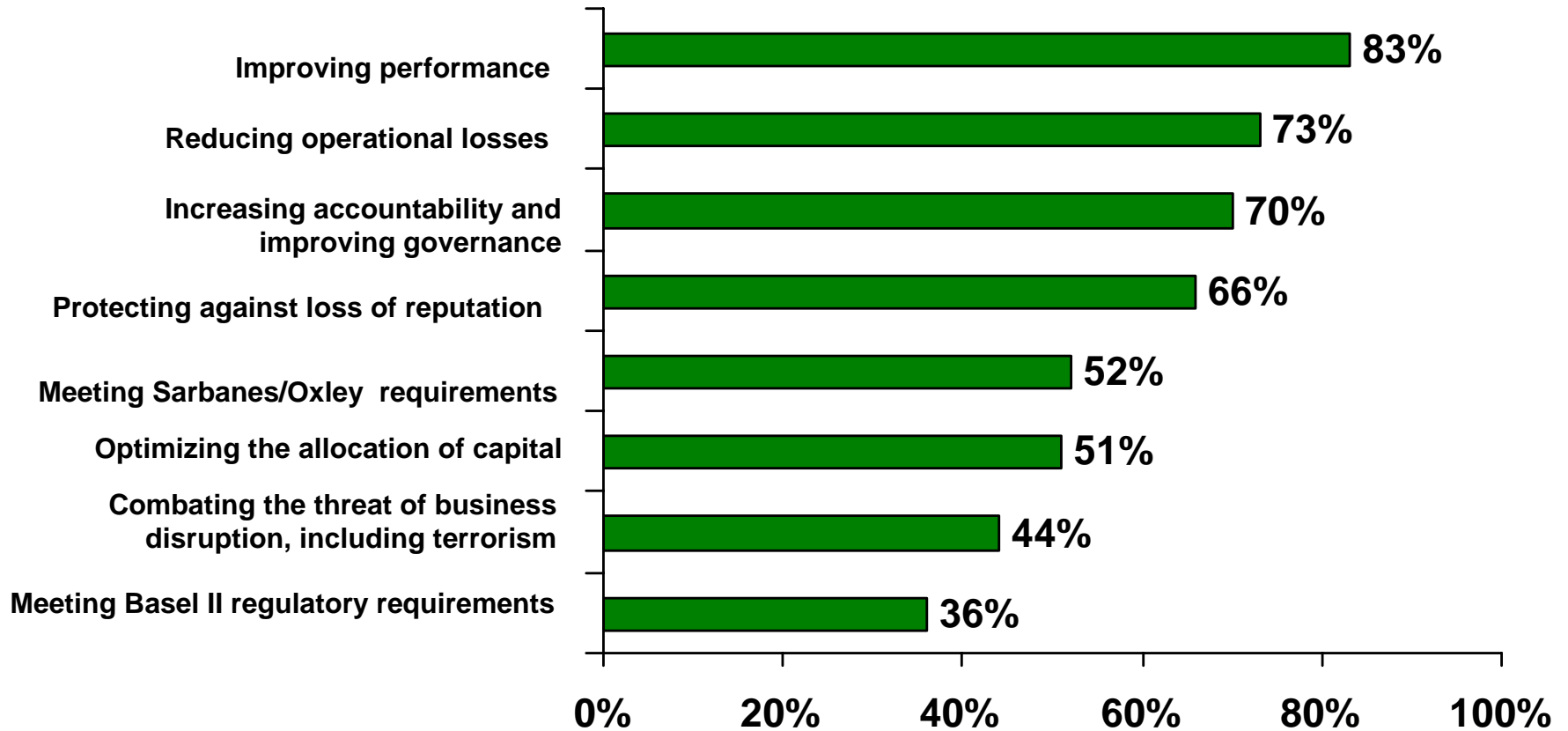


Business Performance Drivers

- Strategy
- Culture
- People
- Structure
- Process
- Reputation



Importance of Business Drivers





Strategy & Culture in business

- Strategy – What is to be done
- Culture – How it is to be done

- This is why the “tone at the top” is key to Risk Assessments and Risk Management



How does security fit in with auditing?

You say: “We need more security or controls”

They hear: “We need another layer of cost and inconvenience.”





Business Directives Requiring Security

- Customer privacy & confidentiality
- Federal, State, Local regulations and legislation
- Transborder data flow
- Acceptable use and content
- Intellectual property & Trade secrets
- Authenticity of electronic records (nonrepudiation)
- Record keeping and audit



Implications for Audits

- Demand for better detection of fraud and illegal acts
- New weapons for detecting fraud
 - Electronic sensors
 - Software agents
 - Computer modeling
 - Triangulation



Implications for Auditors I

- Sharpen skills to include better understanding of:
 - Industries
 - Business systems
 - Business processes
 - Business risks



Implications for Auditors II

- Audit teams will be expanded but specialized
 - Fraud specialist
 - Forensics
 - Regulatory
 - Industrial
 - Information Technology and Systems Development



Implications for Auditors II

- Appropriate approaches needed
- Skills shift from “Getting the bookkeeping correct” to concentrating more on the “tough problems”
- This results in gains in audit efficiency and effectiveness over time
- Findings move from “pass/fail” to specific risk exposures and probabilities
- Auditors will deliver additional value through analysis and interpretation of findings



ERM requires balancing the Hard & Soft sides of Risk Management

Hard Side

- Measuring & Reporting
- Risk oversight committees
- Policies and procedures
- Risk Assessments
- Audit processes
- Systems measurement

Soft Side

- Risk awareness
- People
- Skills
- Integrity
- Incentives
- Culture & Values
- Trust & Communication





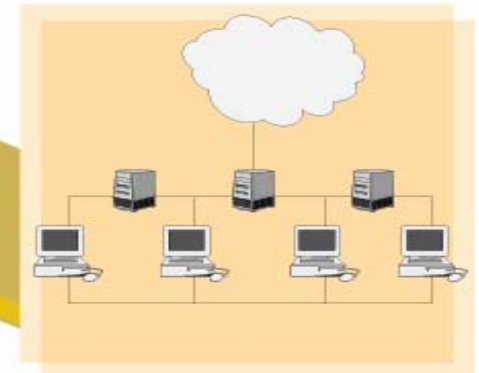
Use Open Communication of Risk Information to Bridge the Gap



Enterprise Management

Business
Planning
Budget

Open Communication



Network

Hack Points
Communication
Systems Administration
Network Support



Summary – Keys to Success

- Senior management commitment
- Support and participation of the IT Security, physical security, audit or other appropriate teams
- Awareness and cooperation of users
- Ongoing assessment of the mission risks
- Competence of the risk assessment team





Lisa Young

813-571-9008 office

813-404-9456 cell

lyoung@brightmsi.com

