Key market drivers have created a “perfect storm” for risk transformation

<table>
<thead>
<tr>
<th>Trends</th>
<th>Challenges</th>
<th>Opportunities</th>
</tr>
</thead>
<tbody>
<tr>
<td>SEC rule changes requiring additional disclosures in proxy and information statements regarding risk, compensation and governance</td>
<td>Not enough resources, competing and multiple risk priorities</td>
<td>Perform enterprise wide diagnostic to understand current risk capabilities</td>
</tr>
<tr>
<td>Rating agency guidelines for evaluating a company’s enterprise risk management practices that impact the organization’s overall credit rating</td>
<td>Creating value from managing risk at an enterprise level</td>
<td>Identify redundancy, overlap and gaps within risk capabilities</td>
</tr>
<tr>
<td>Increased Board and Executive response to regulatory, environment, and market changes</td>
<td>Sustaining consistent, standardized processes to manage risk and measure the effectiveness of risk capabilities</td>
<td>Align risk management capabilities to increase response and agility</td>
</tr>
<tr>
<td>Legal standards, regulatory requirements and increasing third party security requirements</td>
<td>Overcoming barriers that exists from a poor operational performance</td>
<td>Embed effective risk management capabilities into the “rhythm of the business” through inclusion of strategic, financial and operational planning processes</td>
</tr>
<tr>
<td>Elevated conversation of the value risk management can have on strategic and business level performance</td>
<td>Effectively balancing cost associated with managing risk to achieve desired levels of business performance (value)</td>
<td>Reduce the risk and compliance burden at the business level</td>
</tr>
<tr>
<td></td>
<td>Understanding what and how risk should be managed to effectively respond to business demands</td>
<td>Enable technology to create a common standard platform to integrate risk processes</td>
</tr>
<tr>
<td></td>
<td>Emerging technology capabilities</td>
<td>Create a holistic view of risk to address multiple, “silied” risk management practices</td>
</tr>
</tbody>
</table>
Value, cost and risk considerations for implementing risk transformation

A balanced approach to risk transformation

- Execution of a future state will help achieve a sustainable and responsive EGRC organization.
- Integrated and coordination of risk functions drive improved agility and risk response to complex and increasing business challenges.
- Effective risk function/processes that provide increased assurance that governance, risk and compliance objectives are achieved.
- Transformation from a reactive to a proactive risk posture.
- Improved visibility and transparency of risk functions.

- Redundant, duplicative and or overlapping of risk practices across enterprise generate non value-added costs.
- Inefficiency of risk management practices add to overall cost of managing risk.
- Compensation, skills and abilities of resources are unaligned with strategic and business objectives impeding business performance.
- Flexible/variable cost models are not utilized to capitalize on business, organizational and risk management needs.
- Alternative sourcing and resource management strategies are not leveraged or optimized.

- Entity fails to respond to increasing and complex business challenges.
- Risk management practices are not aligned with strategic objectives.
- Unmanaged risks impact reputation, shareholder value and stakeholder relationships.
- Disparate risk functions and lack of discipline in managing risk interdependencies throughout the organization.
- Decision making is not optimized.
- Other business issues have higher visibility resulting in a lack of attention to governance, risk, and compliance related risks.

► Execution of a future state will help achieve a sustainable and responsive EGRC organization
► Integrated and coordination of risk functions drive improved agility and risk response to complex and increasing business challenges.
► Effective risk function/processes that provide increased assurance that governance, risk and compliance objectives are achieved.
► Transformation from a reactive to a proactive risk posture
► Improved visibility and transparency of risk functions.
Coordinate risk functions to reduce overlap, redundancy and decrease costs

Current State

- No documented charters for board or committees
- Board does not have oversight of company identified risks
- Processes not formal to disclose company’s performance with regulatory and compliance stakeholders
- Strategic plan does not support effective governance objectives
- Is the total cost of risk functions at $25 million annually cost effective?
- 13 different risk assessments are performed by various functions
- Technology is not leveraged across risk functions to create efficiencies and reduce costs
- A standard taxonomy for evaluation of risk is not utilized
- Business level controls and processes are not standardized or relevant to meet business objectives
- Risk metrics have not been established and linked to a business and risk strategy
- Improvement programs/initiatives do not include a risk review/assessment

Siloed risk functions reduce value, increase costs, and impact business performance
What is the new risk management?

Current state

<table>
<thead>
<tr>
<th>Board/senior management oversight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit committee</td>
</tr>
<tr>
<td>Risk committee</td>
</tr>
<tr>
<td>Other committees</td>
</tr>
</tbody>
</table>

Siloed risk functions reduce value, increase costs, and impact business performance

Future state

<table>
<thead>
<tr>
<th>Board oversight</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit committee</td>
</tr>
<tr>
<td>Compensation committee</td>
</tr>
<tr>
<td>Risk committees</td>
</tr>
<tr>
<td>Other committee</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Executive management</th>
</tr>
</thead>
<tbody>
<tr>
<td>CEO</td>
</tr>
<tr>
<td>CFO</td>
</tr>
<tr>
<td>CRO</td>
</tr>
<tr>
<td>General Counsel</td>
</tr>
</tbody>
</table>

Aligned mandate and scope

- Coordinated infrastructure and people
- Consistent methods and practices
- Common information and technology
Align and integrate risk activities to improve business performance

**Future State**

- **Board oversight**
  - Audit committee
  - Compensation committee
  - Risk committees
  - Other committee

- **Executive management**
  - CEO
  - CFO
  - CRO
  - General Counsel

**Aligned mandate and scope**
- Coordinated infrastructure and people
- Consistent methods and practices
- Common information and technology

**Increased value, reduced costs, and improved business performance**

- Enhanced board-level reporting and communications
- Enhanced structure to implement risk oversight capabilities
- Processes are formal to disclose company’s performance with regulatory and compliance stakeholders
- Strategic planning supports effective governance objectives
- Total cost of risk functions is reduced from integrating risk functions
- Redundancy, overlap and risk activities are performed in a coordinated manner
- Technology is leveraged across risk functions to create efficiencies and reduce costs
- A standard taxonomy for evaluating risk is utilized
- Business level controls and processes are standardized to support business objectives
- Risk metrics are established and linked to a business and risk strategy
- Improvement programs/initiatives include a risk review and assessment
The future state leverages a holistic, aligned risk performance model

The performance model supports a desired future state

- Governance
  - Board and Management Committees
  - Policies and Procedures
  - Organizational Structure
  - Internal and External Communications
- Risk Management
  - Risk Identification and Assessment
  - Risk Tolerance and Analysis
  - Risk Monitoring
- Integrated GRC Capabilities
  - Mandate
    - Alignment and Coordination
    - Objectives and Values
- People
  - Roles and Responsibilities
  - Competencies and Resources
- Methods
  - Planning and Approach
  - Issue Tracking and Remediation
  - Staffing and Rotation
  - Learning and Development
- Technology Enablement
  - Coverage and Integration
  - Asset Management and Control
  - Communications and Reporting
  - Vendor Management
- Business Level Performance
  - Self Assessment
  - Metrics and Measures
  - Process and Control Optimization
  - Programmed Major Initiatives

Risk transformation embodies a holistic view risk across the organization
Link risk management practices to business planning processes

- **Strategic plan and financial target development**
  - Strategy and Value drivers
  - Long-range strategic plan
  - Strategic risk assessment
  - Strategic initiatives and financial targets
  - Creates enterprise level risk profile aligned to strategy and business objectives

- **Business planning, budget and forecast process**
  - Business-level objectives
  - Detailed planning analysis for business plan
  - Business-level risk assessment
  - Business-level budget, forecast and operating plan
  - Provides basis for structured consideration of risk relative to business plan process

- **Quarterly business performance review process**
  - Quarterly revenue and earnings
  - Quarterly review against business plan
  - Quarterly risk assessment review
  - Business-level performance measurement
  - Routinely challenges the impact of key risks on budget, plan, forecast and performance

- **Ongoing risk & control monitoring and support**
  - Internal audit
  - Regulatory and compliance
  - Internal control (Sox)
  - Other risk and control groups
  - Provides key risk and control groups with routine updates on emerging risk issues
Define the “Rhythm of the Business” and points of integration

<table>
<thead>
<tr>
<th>Q1</th>
<th>Q2</th>
<th>Q3</th>
<th>Q4</th>
</tr>
</thead>
<tbody>
<tr>
<td>JAN</td>
<td>FEB</td>
<td>MAR</td>
<td>APR</td>
</tr>
<tr>
<td>1/xx</td>
<td>4/xx</td>
<td>7/xx</td>
<td>10/xx</td>
</tr>
</tbody>
</table>

Board and audit committee meetings
- Risk update and IA plan review
- Strategic and Value drivers
- Long-range strategic plan

Executive-level strategy
- Strategy and Value drivers
- Long-range strategic plan
- Strategic initiatives & financial targets

Business-level planning
- Business-level objectives
- Planning analysis for business plan

Quarterly business review
- QBR risk review

Regulatory and compliance
- Quarterly ECC

Internal audit
- Quarterly updated

Internal financial controls (SOX)
- Quarterly 302/404 certification process

Monthly/quarterly close
- 1/xx
- 2/xx
- 3/xx
- 4/xx
- 5/xx
- 6/xx
- 7/xx
- 8/xx
- 9/xx
- 10/xx
- 11/xx
- 12/xx

Ernst & Young
Quality In Everything We Do
Representative organizational structure – Example 3

Integrated Risk and Compliance Functions Coordinated Under Global Chief Compliance Officer With Direct Reporting To The CFO and AC
Observations and other considerations
The risk transformation strategy roadmap

Identify/Diagnose
Phase I

1. Plan and mobilize
2. Assess risk management culture
3. Understand current risk capabilities (high level)
4. Identify redundancy, overlap and duplication
5. Assess risk reporting frequency and performance
6. Identify high level risk spend (costs)
7. Assess risk process maturity
8. Assess coordination/integration maturity
9. Assess GRC capability maturity
10. Identify gaps to achieve future state
11. Establish a business case and roadmap for change

100 day Implement

1. Plan and Mobilize
2. Adopt a common risk framework
3. Assess risk strategy
4. Identify and review business and GRC objectives
5. Define governance model (Board/executive level risk oversight)
6. Define risk appetite (sufficient to support the business case)
7. Assess risk (Risk assessment-condensed)
8. Document rhythm of the business and integration points (effectiveness, efficiency and agility)
9. Assess risk management model
10. Design/Revise Reporting (Board/executive level)
11. Demonstrate technology enablement
12. Validate target pilot for Phase I
13. Develop a business case and roadmap

Design/Deliver
Phase I

100 day
Launch

1. Plan and mobilize
2. Identify focused initiatives
3. Enable risk culture
4. Operationalize effective reporting to the board
5. Refine Risk Appetite
6. Refine risk governance model
7. Embed risk capabilities into the business
8. Pilot risk integration across processes, functions or domain
9. Pilot an enabling technology to support risk integration across processes, functions, or domain
10. Implement other initiatives (opportunities to reduce costs, improve efficiency or enhance GRC capabilities)

Design/Deliver
Phase II

1. Roll-out risk integration enterprise-wide
2. Institutionalize self-assessment at the business level
3. Implement formal policies and procedures, communication strategy, cascade a technology initiative
4. Develop/validate risk and control measures
5. Continue to coordinate interactions with business units to achieve “risk convergence”
6. Migrate manual processes to automated processes to gain leverage and efficiency through the use of IT
7. Create common data structure across enterprise to allow efficient sharing of risk and control information
8. Establish risk data analytics/predictive modelling to proactively manage risk
9. Evaluate continued relevance of risks, competencies and risk processes given changes in the business
10. Beyond (enterprise-wide)

100 day
Beyond

1. Roll-out risk integration enterprise-wide
2. Institutionalize self-assessment at the business level
3. Implement formal policies and procedures, communication strategy, cascade a technology initiative
4. Develop/validate risk and control measures
5. Continue to coordinate interactions with business units to achieve “risk convergence”
6. Migrate manual processes to automated processes to gain leverage and efficiency through the use of IT
7. Create common data structure across enterprise to allow efficient sharing of risk and control information
8. Establish risk data analytics/predictive modelling to proactively manage risk
9. Evaluate continued relevance of risks, competencies and risk processes given changes in the business

Value to the business
Representative established organizational structure

*Aligned and Coordinated Risk, Control and Compliance Functions Coordinated Under CFO, CRO and Corporate Counsel with integrated reporting to the CEO and Audit Committee*
Representative organizational structure – Example 2

Representative Advanced Organizational Structure

Aligned and Coordinated Risk, Control and Compliance Functions Coordinated Under CFO and Corporate Counsel with integrated reporting to the CEO, Audit Committee and the Board of Directors

Board of Directors

CEO

Audit Committee

Chief Risk Officer

Corporate Counsel

CFO

Business Unit Leadership w/ "Risk Champions"

Enterprise Risk Mgmt.

Compliance

Internal Control (Sox)

Internal Audit

Annual Plan and Quarterly Business Reviews

Ongoing Risk Assessment & Monitoring

Corporate Ethics & Compliance Program

Monthly and Quarterly Close with Control Assessment

Annual Audit Plan Based On Enterprise Risk Profile w/ Quarterly Updates

ERNST & YOUNG
Quality In Everything We Do