Enterprise Reputation and Risk Management (ER²M) Overview

N. C. State University ERM Initiative Roundtable Series

October 3, 2008

Jim Traut
Director ER²M
Agenda

- Background on Heinz
- Business case for ERM
- Organization structure
- Risk Governance Framework and Management Model
- Risk assessment processes
  - Top-down
  - Functional area
- Summary and communication of risks
- Risk mitigation continuous improvement approach
- Lessons learned
You May Know Heinz by our Leading Branded Products

Top 15 Brands Generate Almost 70% of Total Sales

* Refer to Trademark Notices on page 38

Heinz Across the Globe

- Annual sales exceeding $10 Billion
- Enterprise value of approximately $20 Billion
- Over 30,000 employees
- 50 Business Unit offices
- Multiple ERP systems
- 75 factory locations worldwide
- Over 16,000 product stock keeping units (SKUs)
- 55% of our sales are from products manufactured and sold internationally
Heinz Mission Statement and Values

MISSION STATEMENT
As the trusted leader in nutrition and wellness, Heinz — the original Pure Food Company — is dedicated to the sustainable health of people, the planet and our Company.

VALUES

Team Building & Collaboration
Embraces great ideas from everywhere and respects all individuals.

Vision
Defines a compelling, sustainable future and creates the path to achieve it.

Innovation
Spots consumer & customer needs and meets them with simple, creative solutions.

Results
Delivers on commitments, takes accountability and balances the short- and long-term.

Integrity
Always tells the truth, acts with the highest ethical standards and ensures that our products are of the highest quality.
Henry John Heinz Founded Heinz in 1869

Nearly 140 years ago, our culture was built upon the fundamentals driven by our Founder’s favorite motto:

“To do a common thing uncommonly well brings success”
Today the Vision and Culture Continues

Bill Johnson, our 6\textsuperscript{th} Chief Executive Officer in 140 years leads Heinz with the mission that:

“Heinz wants to be the most trusted company in the industry”

ER\textsuperscript{2}M has been positioned as an enabler to:

- Further support doing the common thing uncommonly well
- And to help us become the most trusted food company
Risk Management Historically

- Historically, risk was one of many considerations in every day business activities and decision making

- Risk assessments and risk considerations were informally addressed by management without standard processes

- Risk was many times associated with:
  - Insurance management
  - Controls
  - Prevention
  - Strength, Weaknesses, Opportunities and Threats analysis (SWOT)
  - One-time negative events that caught management by surprise
Risk Management Evolution

Risk Management and operational transparency have moved up on the agendas of Fortune 500 Board of Directors and Chief Executive Officers for many reasons including:

- High profile business failures due to accounting or trading frauds
- Terrorist events that have crippled businesses
- Natural disasters that shed light on inadequate business continuity preparedness
- Significant product recalls and resulting reputation and brand damage
- Credit crisis and increased commodity volatility
- Investor rating and credit rating services are including Enterprise Risk Management (ERM) in their evaluation criteria (i.e., Standard and Poor’s)
- Customer expectations of a reliable supply chain
- Increasing insurance costs
- Potential liability associated with not adequately carrying out fiduciary responsibilities
- Answering the question “What else keeps you up at night?”
Closer to Home

List risks and events experienced by your company in these areas:

- **Operational Risk Areas**
  - Employee Safety Processes
  - Product Safety and Quality
  - Asset Conservation
  - Environmental Management
  - Facility and Product Security
  - Information Services
  - Human Resources

- **Non-Operational Risk Areas**
  - Strategic & Marketing
  - Corporate Governance & Ethics
  - Financial
  - Legal
  - Information Services
  - Human Resources
Standard & Poor’s* ERM Analysis of Credit Ratings

For several years, S&P’s analyzed ERM for financial industry firms.

- November 15, 2007 – S&P’s Request for Comment: Enterprise Risk Management Analysis for Credit Ratings of Non-Financial Companies
- May 7, 2008 – Enterprise Risk Management: Standard & Poor’s To Apply Enterprise Risk Analysis To Corporate Ratings
  - S&P to incorporate ERM into review meetings (third quarter 2008)
  - Within one year, S&P expects all companies to have at least one initial ERM discussion with their analysts
  - ERM analysis to be included in S&P reports (fourth quarter 2008)
  - Likely scoring system is Excellent/Strong/Adequate/Weak
    - Note the ERM findings in 2006 of 241 insurers – Excellent (3%), Strong (10%), Adequate (82%) and Weak (5%)
S&P’s ERM Impact

- In the near to long term, companies can continue to further develop an open risk aware vs. risk adverse culture that:
  - Supports risk/reward ownership, consideration, actions and processes
  - Maintains focus upon reputation, brand and business building and protection of Enterprise Value
  - Creates additional risk/reward awareness and transparency deeper into:
    - Strategies
    - Business Unit objectives and processes
    - Functional and cross-functional areas

- As S&P develops an ERM knowledgebase by industry and begins to publish comparison ratings:
  - Companies can continue to drive ERM for competitive advantage (see The ERM Imperative)
What Has Changed Recently?

Areas attracting increased management attention/concern:

<table>
<thead>
<tr>
<th>RISK AREA</th>
<th>ACTIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commodity Management &amp; Price Volatility</td>
<td></td>
</tr>
<tr>
<td>Credit Market Volatility</td>
<td></td>
</tr>
<tr>
<td>Economic Slow Down</td>
<td></td>
</tr>
<tr>
<td>Food Safety</td>
<td></td>
</tr>
<tr>
<td>Sustainability</td>
<td></td>
</tr>
</tbody>
</table>
ER²M Priorities to Date

Our ER²M priorities to date have been focused upon:

- Establishment of ER²M structure (Office of Risk Management)
- Development of Heinz ER²M Methodology
- Conducting top down risk assessments
- Mitigation of top 12 risks
- Standardization of Operational Risk Areas global:
  - Risk assessment approach
  - Common ways of working
  - Key Performance Indicators
  - Scorecards
In May 2006, Heinz initiated a broader integrated operational approach to the Enterprise Reputation and Risk Management function and the Office of Risk Management was established at World Headquarters under a Senior VP.
Key ER²M Interactions

Continued focus on FCPA 1977 and Sarbanes-Oxley Act of 2002

Ongoing Risk Oversight

Ensure Global Risk Ownership

Input into 10K and 10Q Risk Factors

Identify & Prioritize Risks

Include Key Risks & Resources

Align Risk Appetite with Controls

Input into Annual Audit Plan

Continuous Improvement (Process Transformation through Collaboration)

BOD (Audit Committee)

Office of the Chairman & Presidents Council

Disclosure Committee

Functional Areas & Business Units

Strategic Planning & Annual Operating Plan

Process Improvement & Operational Compliance

Corporate Audit

SEC, PCAOB, NYSE & rating agencies require or encourage risk management-related activities
The ER²M Imperative

The purpose of Enterprise Reputation and Risk Management is to protect and thereby maximize Heinz Enterprise Value and Brand Equity:

- Company Reputation and Brand Image
- Product Quality and Safety
- Employee Health and Safety
- Talent
- Physical Assets
- Processes and Systems
- Customers and Suppliers
- Other Intangible Assets (i.e., Trademarks, Consumer and Customer Relationships)

Through collaboration across functional areas and geographic regions:

- Generate awareness and identify potential risks and opportunities
- Evaluate and establish acceptable risk tolerance levels
- Ensure alignment of Heinz Policies, standards and best practices
- Facilitate development of risk mitigation solutions and measurement

In order to ensure the achievement of the Company’s objectives and the long-term sustainability of the enterprise.

ER²M = Competitive Advantage
Enterprise Risk Management Defined

ERM as Defined by COSO:
A process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.

ERM Application at Heinz:
We will establish a unified, global, cross-functional approach to identify, prioritize, measure and manage key business risks.

- The ERM function will drive global facilitation, best practices, compliance and continuous improvement

- The accountability for and ownership of risks and mitigation plans will remain with the appropriate Business Unit and World Headquarters management, shared with global process owners

- A common integrated global process will be used to manage risks and mitigation activities across all risk areas
Global and Business Unit Level Risk:

1. **Awareness** – realize existence of events that could prevent Company from achieving objectives

2. **Measurement** – analyze likelihood and impact of events

3. **Prioritization** – rank events cross-functional and across enterprise

4. **Action** – take active steps to mitigate or purchase insurance

5. **Integration** – build mitigation processes into ways of doing business

6. **Culture** – continuous process of 1-5 above
Bringing Order to ERM Complexity

Classification of risk into 3 Major Risk Areas:
- Management Leadership
- Operational (Supply Chain)
- Foundation Functional

Each risk has a rating based upon:
- Likelihood of occurrence
- Impact (cost to Heinz)
- Level of control activities

Risks are managed by:
- Process improvement to prevent or reduce probability and impact
- Purchasing insurance to reduce financial impact

Residual Risk (the risk remaining after mitigation) will always be present and should be evaluated based upon cost/benefit analysis
Risk Governance Framework

Reputation (CEO, Officers, BU Presidents, and Board of Directors)

Management Leadership Risk Areas

Strategic (Office of the Chairman)

Corporate Governance And Ethics (Vice President)

Market (Office of the Chairman)

Operational (Supply Chain) Risk Areas

Quality (Vice President)

Environmental & Sustainability (Director ORM)

Health & Safety (Director ORM)

Security (Director ORM)

Business Continuity Operations (Director ORM)

Asset Conservation (VP Insurance/ Director ORM)

Foundation Functional Risk Areas

Financial, Including SOx (Chief Financial Officer)

Legal (General Counsel)

Information Services (Chief Information Officer)

Human Resources (Chief People Officer)

Continuous Process Improvement - All WHQ and BU Employees

Insurance of Risk - (Limits Financial Impact of Risk) – VP Insurance
Heinz Risk Management Model

Operational Risk Areas
- Heinz Safety Process
- Food Quality and Food Safety
- Asset Conservation
- Environmental Management System
- Facility Security and Food Defense
- IS
- HR

Non-Operational Risk Areas
- Strategic & Market
- Corporate Governance & Ethics
- Financial
- Legal
- Insurance
- IS
- HR

Values
- Protect Employees, Products and Assets
- Promote Ethical and Legal Behavior
- Protect Shareholder Interests
- Protect All Heinz Brands and Market Positions
- Maintain the Flow of Goods to Heinz’ Customers
- Build Social, Environmental and Economic Sustainability
- Continuous Improvement of Heinz Processes
Global Risk Assessment Process

- We refined the risk inventory for each functional area
  - From brainstorming list to top three to five critical risks based upon:
    - Risk data
      - Risk
      - Functional Risk Area and Ownership
      - Risk Classification
    - Control Activities
      - Policies
      - Procedures/processes
      - Scorecards/measurements
      - Monitoring
    - Risk ranking score
      - \((\text{Likelihood} + \text{Impact})/2 = \text{Risk Score}\)
      - Control Effectiveness Level - \((\text{Likelihood} + \text{Impact})/2 = \text{Net Risk Score (Gap)}\)
        - Each criteria is based on a five point scale
        - Scale includes quantitative and qualitative ranking criteria
    - Recommendations for filling gap
      - Validated findings with executive risk owner in each functional area
      - Validated list reviewed with Risk Council
      - Top risks and mitigation efforts reviewed with senior management
      - Annual process
Risk Score Equation

The following approach is used to facilitate identification of top Company risks:

\[
\text{Risk Score} = \frac{\text{Likelihood} \times \text{Impact}}{2}
\]

- Little or no Consideration Of Control

\[
\text{Control Level} - \text{Risk Score} = \text{Gap}
\]

+ Gap means controls are adequate
- Gap means controls should be reviewed
**Filling in the “Gap”**

For each critical risk identified, we consider current mitigation processes and the level of risk we are willing to accept. If there is a gap between the risk we are willing to accept and the current mitigation processes in place, we strive to optimize risk coverage by filling in the gap with new or improved mitigation processes or insurance coverage.
Resolver Ballot* Sessions

- Resolver Ballot handheld voting enabled us to interactively assess our top-down global risks in order to generate consensus in key areas and/or discover deficiencies.

- In each Resolver Ballot risk assessment session, functional leads:
  - Reviewed each functional risk from a strategic perspective (3 year time frame)
  - Considered controls based upon current implementation
  - Voted on each risk separately, based on a five point scale for three criteria:
    - Likelihood
    - Impact
    - Control

Annual top-down risk assessment:
- Numerous interactive risk assessment meetings with WHQ and limited BU management
- Identified, ranked and validated risks
- Risk inventory refined to top risks based upon risk Gap scores

* Resolver Ballot is a registered trademark of Resolver Inc.
## Top Assessed Risks

Top risks are presented in the following manner based upon the Risk Gap scores:

<table>
<thead>
<tr>
<th>Risk</th>
<th>Actions</th>
<th>Global Owners</th>
<th>Process Owners</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Note: Risk mitigation efforts are monitored via scorecards for functional risk areas.
Risk Appetite Management Model

The risk assessment process for a global company is not exact. Regardless of the methods used to gather risks, the Company should define their Risk Appetite – how much risk the Company is willing to accept after mitigation.

**Higher Risk Appetite Risks** - Company is willing to accept more risk for the potential rewards

**Lower Risk Appetite Risks** - Company is unwilling to accept more risks due to potential negative consequences

If the risk assessment indicates a difference between the residual risk and the Risk Appetite, mitigation efforts should be adjusted to match the level of controls with the Risk Appetite.

Our Risk Appetite Management Model summarizes functional risk categories based upon the Company’s perceived current risk appetite. Risks that have Gaps that do not match our Risk Appetite are indicated by an arrow and the targeted Risk Appetite level.
## Risk Appetite Management Model

Risk Appetite defines the Company’s willingness to accept risk after mitigation

<table>
<thead>
<tr>
<th>Risk Appetite</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Higher Risk Appetite</strong></td>
<td>(Willingness to Accept More Risk for Reward)</td>
</tr>
<tr>
<td><strong>Medium Risk Appetite</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Lower Risk Appetite</strong></td>
<td>(Unwilling to Accept Risk Due to Potential Consequences)</td>
</tr>
</tbody>
</table>

▲, ▼ - indicates the targeted direction of Risk Appetite

H, M, L - Higher, Medium, Lower indicates the targeted level for Risk Appetite
Heinz Risk Classification Summary

To summarize the risks for the broader communication and benefit of Heinz WHQ and BU Management, each risk was assigned a functional area classification.

This Risk Classification Summary should be used as a reminder of the important considerations that should be included in the daily management of our businesses.

For each risk classification, management can ask the question “How effective are the … risks in our functional area or at our Business Unit?”
# Heinz Risk Classification Summary

<table>
<thead>
<tr>
<th>Management Leadership</th>
<th>Supply Chain</th>
<th>Security</th>
<th>Legal</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Strategic</strong></td>
<td><strong>Quality</strong></td>
<td><strong>Business Continuity Planning</strong></td>
<td><strong>Human Resources</strong></td>
</tr>
<tr>
<td><strong>Corporate Governance &amp; Ethics</strong></td>
<td><strong>Environmental &amp; Sustainability</strong></td>
<td><strong>Asset Conservation</strong></td>
<td><strong>Information Services</strong></td>
</tr>
<tr>
<td><strong>Market (Sales &amp; Marketing)</strong></td>
<td><strong>Health &amp; Safety</strong></td>
<td><strong>Financial</strong></td>
<td></td>
</tr>
</tbody>
</table>
In Q4 each year an independent RMP assessment is completed at each factory/facility to:
  • Determine the site’s compliance to the standards
  • Generate a score called the Risk Control Rating (RCR)

Upon completion of the assessment a prioritised improvement plan is generated. The plan includes the specific Standards the site needs to work on to manage each risk area. A Target Risk Control Rating (RCR) is generated. The RCR is included in the site management team’s objectives.

The site work throughout the year to implement the improvements as well as maintaining controls already implemented.

The site completes a formal end of year review.
Critical we get risk assessment right.

Risk assessment determines the physical controls, ways of working and training we must implement to eliminate or reduce the risks.

It also determines the monitoring, validation and verification required.
FY09 and Beyond

Embed ER²M into additional Heinz ways of working via:

- Further develop a risk aware vs. risk adverse culture:
- Refine annual top-down risk assessments to include:
  - Broader functional and Business Unit input
  - Emerging and leveraged risks
- Drive improvements in functional risk scorecard measures
- Evaluate S&P’s recently issued ERM credit rating criteria in preparation for Company review
Global ER²M Strategy and Activities

- Year 1: Developed ER²M Approach
- Year 2: ORM Integration
- Year 3: ORM Refinement Non-ORM Risk Awareness
- Years 4-5: Achieve Best in Class Status
Top 10 ERM Lessons Learned

1. Board of Director and Executive Level support is critical for success
2. Establish Risk Management ownership by functional area
3. Encourage open discussions of “what keep people up at night”
4. Convert initial lists of “worries” to actionable risks
5. Respect and protect anonymity of Risk Assessment participants
6. Communicate regularly, thoroughly and top to bottom
   – Office of Chairman and Audit Committee – semiannually
   – Summarize Top Risks and Mitigation Requirements
   – Memos to Business Unit Presidents, CFOs and Management Teams
7. Measure risk mitigation efforts via scorecards
8. ERM has to be customized to your culture and ways of working
9. ERM is a cultural journey rather than a project destination
10. ERM drives synergies as the whole is greater than the sum of the parts
Heinz has done the common thing uncommonly well for nearly 140 years.

Let’s maintain our sustainability throughout the next century!
Trademark Notices

Boston Market is a registered trademark of Boston Market Corporation used under license.

WEIGHT WATCHERS on foods and beverages is the registered trademark of WW Foods, LLC and is used under license. WEIGHT WATCHERS for services and POINTS are the registered trademarks of Weight Watchers International, Inc. and are used under license.

T.G.I. Friday's is a trademark of TGI Friday's of Minnesota, Inc. and used under license by H.J. Heinz Company, L.P. © TGI Friday's Inc. 2008.