Records and Information Management:

*Managing the Real Risks Facing Your Organization*

By:
Christine White and Emily Bone
Molson Coors Brewing Company

MOLSON COORS BREWING COMPANY

• 19 Breweries in Canada, U.K., Central Europe, China, and India
• Over 100 brands in portfolio
• Provides beer to over 50 countries

“Delighting the world’s beer drinkers”
Agenda

1. Identifying and assessing organizational risks related to records and information management
2. Global challenges, considerations, and mitigation strategies
3. Managing the risk: controls and education

Identifying & Assessing Organizational Risks Related to Records and Information Management
Identifying & Assessing Risks Related to RIM

• What are risks with Records Management
• Case studies / records in the news
• Regulations & standards
• M & A / Due Diligence

What are risks in Records Management?

• What is the risk?
• Value of identification
• Managing risk
  – Holistic and systematic
  – Risk management program

Ad Hoc  Awareness  Monitoring  Formalizing  Mature
Case Studies / History of Records

- Zubalake vs. UBS
- Arthur Anderson / Enron
- Records in the News

Regulations & Standards

- ISO 15489
- The Principles
- Sarbanes Oxley
- H.I.P.P.A.
- F.R.C.P. Rule 26
- Data Protection Directive
- Personal Information Protection and Electronic Documents Act
ISO 15489

- International Organization for Standardization
  - 1st International Standard devoted to Records Management
  - Companies in compliance are following standards and best practices
  - Part I and Part II in standard(s)
    - Part 1 = General overview
    - Part II = In-depth practicalities of Records Management

The Principles

- Published by ARMA International
  - Not-for-profit professional association & authority on managing records & information
- Comprehensive in scope, general in nature
- Fosters awareness & standards to assist organizations
- Total of eight (8) Principles
- Maturity model has Levels 1 - 5
GARP Principles

1. Accountability  
2. Transparency  
3. Integrity  
4. Protection  
5. Compliance  
6. Availability  
7. Retention  
8. Disposition

The Principles

1. Accountability
The Principles

2. Transparency

3. Integrity
The Principles

4. Protection

The Principles

5. Compliance
The Principles

6. Availability

7. Retention
The Principles

8. Disposition

Sarbanes Oxley (SOX)

- United States Federal Law
- Became law in 2002
- New / enhanced standards for all U.S. public company boards, management & public accounting firms
H.I.P.A.A.

- **Health Insurance Portability and Accountability Act of 1996**
  - Title I & Title II

F.R.C.P. Rule 26

- Federal Rules of Civil Procedure Rule 26
  - Duty to Disclose; General Provisions Governing Discovery
Data Protection Directive

• Protection of individuals with regard to the processing of personal data / free movement of such data

• Important component of EU privacy and human rights law

P.I.P.E.D.A.

• Personal Information Protection and Electronic Documents Act (PIPEDA)

• Canadian law relating to data privacy
Mergers & Acquisitions

• Policies
• Retention Schedules
• Financial department
• Cultural
• Language
• Use The Principles for due diligence
• Country specific regulation(s)

Global Challenges, Considerations & Mitigation Strategies
Global Challenges, Considerations & Mitigation Strategies

- Multiple languages across business
- Conflicting regulations
- Retention Schedules
- Global policies
- Legal holds
- Business Continuity Management

MULTIPLE LANGUAGES
Conflicting Regulations

- Retention
- Privacy laws vary
- Union vs. non-union
- History / case studies

Retention Schedules

- Currently 3 different schedules
  - Canada
  - U.K.
  - U.S.
Global Policies

<table>
<thead>
<tr>
<th>MOLSON Coors</th>
<th>Title:</th>
<th>Global Records Management Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>MOLSON Coors</td>
<td>Title:</td>
<td>Information Classification Policy</td>
</tr>
<tr>
<td>Molson Coors Brewing Company Policy</td>
<td>Scope:</td>
<td>Enterprise-wide and applies to all of MCBC and its contractors (and their employees) who handle MCBC information</td>
</tr>
<tr>
<td>MOLSON Coors</td>
<td>Title:</td>
<td>Information Technology (IT) Use</td>
</tr>
<tr>
<td>Molson Coors Brewing Company Policy</td>
<td>Scope:</td>
<td>Enterprise-wide</td>
</tr>
<tr>
<td>Owner:</td>
<td>MCEC Information Technology Security Officer</td>
<td></td>
</tr>
<tr>
<td>Effective Date:</td>
<td>27 September 2011</td>
<td></td>
</tr>
</tbody>
</table>

Molson Coors Brewing Company (MCBC) provides employees and third parties with information technology and systems for business use. This policy details the acceptable use of these Information Technology (IT) assets.

Legal Holds

- IT, Legal, Records, etc. involved
- Formal process
- Senior support
- Privileged and confidential different in each county
Business Continuity Management

• 2012 Business Continuity Program started
• Upper management support
• BIA completed
• BCP created by function
• Interviews / exercises

Vital Records - BCP
Managing the Risk: Controls & Education

- Senior leadership support / Steering Committees
- Clean Out Day
- Global Information Classification Policy
- Translations
- Internal Audit ‘can be your friend’
Senior Leadership Support / Steering Comm’s

- Right people involved with right work
- Upper level support

Annual Clean Out Day

- U.S. and Canada currently, U.K. in future
- In the U.S. – Annually
  - 2009 = Paper focused
  - 2010 = Electronic focused
  - 2011 = Paper & electronic focused
- Volunteer quad leaders
- Contests and prizes
- True ‘team’ event that involved all functions
- Opportunity to train / educate users
Annual Clean Out Day (cont’d)

- Canada
  - Bi-annually
  - Similar process with great results
- U.K.
  - Records Coordinators implementation
  - 1st Clean Out Day in 2013

Global Information Classification Policy

- Instructions on how to mark company records
  - Public, Internal Use Only, Confidential, Highly Confidential

<table>
<thead>
<tr>
<th>Description</th>
<th>PUBLIC</th>
<th>INTERNAL USE ONLY</th>
<th>CONFIDENTIAL</th>
<th>HIGHLY CONFIDENTIAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routine availability of information through public sources and company websites.</td>
<td>Not generally identified or known outside the enterprise.</td>
<td>Disclosure may cause moderate enterprise or individual damage, loss of shareholder confidence and temporary drop in stock value.</td>
<td>Disclosure may cause regulatory or contractual liabilities, reputation or public image damage, loss of customers and business partners, and drop in stock value.</td>
<td></td>
</tr>
<tr>
<td>Suitable for public distribution.</td>
<td>Provided freely to internal employees via the company’s intranet and other means. This information is to be disclosed to third parties, generally, only if a confidentiality agreement has been signed.</td>
<td>Tightly controlled and restricted based on the concept of “need to know”. Disclosure requires the Information Owner’s approval and, in the case of third parties, generally, a signed confidentiality agreement.</td>
<td>Limited to specified individuals designated by the Information Owner. No copying (electronic or paper) is permitted without Information Owner approval. All electronic and paper copies must be marked <strong>HIGHLY CONFIDENTIAL</strong>. Signed confidentiality agreement generally required.</td>
<td></td>
</tr>
</tbody>
</table>
Translations

- Global policies translated into all applicable languages

<table>
<thead>
<tr>
<th>MOLSON Coors Brewing Company Policy</th>
<th>Title:</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner: Global Records Management</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MOLSON Coors Brewing Company Policy</th>
<th>Title:</th>
<th>宣传文责任政策</th>
</tr>
</thead>
<tbody>
<tr>
<td>负责人： MOLBC 公司企宣部</td>
<td></td>
<td></td>
</tr>
<tr>
<td>公告日期： 2010年10月13日</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Internal Audit can be your friend!

- Can identify risks in audits
- Can help train / educate / pass company info to department’s
Conclusion

• Learn from the past
• Follow applicable laws
• Take steps to protect / eliminate risk
• Put the right people in the right places
• Be visible & available
• Do your research
• Use experts

Questions
Thank You!