## Risk Exercise: Sample Risk Assessment

<table>
<thead>
<tr>
<th>Level</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>CORRUPTION/BRIBERY</td>
<td>INCENTIVE PROGRAM</td>
<td>RECORDS RETENTION</td>
</tr>
<tr>
<td></td>
<td>PRIVACY/DATA PROTECTION</td>
<td>CONFLICTS OF INTEREST</td>
<td>SOCIAL MEDIA</td>
</tr>
<tr>
<td></td>
<td>CULTURE/TONE</td>
<td></td>
<td>ANTITRUST/COMPETITION LAW</td>
</tr>
</tbody>
</table>
Risk Exercise: Sample Heat Map

EXAMPLE
1 – Corruption/Bribery
2 – Privacy/Data Protection
3 – Culture/Tone
4 – Incentive Program
5 – Conflicts of Interest
6 – Records Retention
7 – Social Media
8 – Antitrust/Competition Law
## Risk Exercise: Sample Risk Mitigation

<table>
<thead>
<tr>
<th>PRIORITY</th>
<th>RISK/ISSUE</th>
<th>SAMPLE HIGH-LEVEL MITIGATION STRATEGIES</th>
</tr>
</thead>
</table>
| 1        | CORRUPTION/BRIBERY | - Identify industry compliance failures in areas of corruption/bribery and present risks/trends to senior leaders along with mitigation plan  
- Develop/implement policies and procedures for Anti-Corruption/Bribery Program to include Due Diligence practices when engaging with vendors and third-parties  
- Develop and deliver focused training/awareness on anti-corruption/bribery topics throughout the organization to include third-parties  
- Incorporate Company compliance standards into all third-party contracts  
- Establish process for ongoing monitoring and auditing of Program effectiveness |
| 2        | PRIVACY/DATA PROTECTION | - Engage qualified experts to review and assess full scope of breach and related impact/liabilities; leverage third-party external support  
- Identify systemic root cause of breach; report/disclose as appropriate  
- Establish and implement internal controls to manage/mitigate risk area moving forward (e.g., technology controls, policies, procedures, training, software)  
- Identify/recruit fully qualified internal resource to lead and manage Company risk area; vet qualifications consistent with acceptable standards/best practices |
| 3        | CULTURE/TONE | - Establish board/leadership training and awareness activities; focus on oversight responsibilities, tone, E&C program effectiveness, etc.  
- Present value proposition and needs for E&C Program; secure adequate resources  
- Conduct a Company-wide culture assessment to understand current state; establish plan/process for ongoing monitoring and assessment activities  
- Develop/integrate a new Code of Conduct to include training of employees at all levels of the organization; facilitate/establish a Company Values Statement |
<table>
<thead>
<tr>
<th>PRIORITY</th>
<th>RISK/ISSUE</th>
<th>SAMPLE HIGH-LEVEL MITIGATION STRATEGIES</th>
</tr>
</thead>
</table>
| 4       | COMPANY INCENTIVE PROGRAM   | o Review/assess current state of Company incentive program to include parties involved in development/management, processes, protocols, launch, communications, and results/metrics to date *(payouts, accounts opened, etc.)*  
       |                              | o Engage with leadership on related E&C risks and potential likelihood/impact to organization; recommend modifications/changes to existing program  
       |                              | o Implement independent E&C oversight and management protocols and controls to prevent potential wrongdoing and mitigate risk; includes ongoing monitoring  
       |                              | o Ensure E&C participation/input on all Company incentive programs moving forward |
| 5       | CONFLICTS OF INTEREST       | o Inventory existing *(potential)* COI issues and create mitigation plans  
       |                              | o Establish policies and procedures for addressing and managing conflicts of interest to include proper reporting channels, review, waivers, etc.  
       |                              | o Develop/implement a process for ongoing COI disclosures and related management  
       |                              | o Review global COI policies for cultural considerations and assure consistency with corporate level polices and procedures  
       |                              | o Implement Company-wide training and awareness program focused on COI |
## Risk Exercise: Sample Risk Mitigation

<table>
<thead>
<tr>
<th>PRIORITY</th>
<th>RISK/ISSUE</th>
<th>SAMPLE HIGH-LEVEL MITIGATION STRATEGIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>RECORDS RETENTION</td>
<td>o Inventory existing policies and procedures by business unit; evaluate consistencies, practices, etc., across the organization</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Determine if any existing practice or past action has resulted in a violation of law</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Secure resource(s) to lead/implement a centralized RIM Program and infrastructure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Establish centralized policies and procedures related to RIM and retention standards</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Implement/deliver applicable training and awareness across the organization regarding RIM policies, practices, expectations, etc.</td>
</tr>
<tr>
<td>7</td>
<td>SOCIAL MEDIA</td>
<td>o Evaluate existing uses of social media for business purposes to include impact, media sources, use of Company assets, and employees involved</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Establish Company-wide policy/procedure regarding the use of social media during work hours (<em>both for business and personal purposes</em>); implement policy/procedure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Provide Company-wide training/awareness regarding policy, expectations, etc.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Establish appropriate technology controls and related risk mitigation efforts</td>
</tr>
<tr>
<td>8</td>
<td>ANTITRUST / COMPETITION LAW</td>
<td>o Engage with leadership; recommend immediate cancellation of upcoming rally</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Review/investigate history and current state of proposed rally with competitors; includes parties involved, any past meetings, potential wrongdoing, etc.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Establish/implement Company-wide policy/procedures regarding direct and indirect interaction/engagement with competitors and related risks</td>
</tr>
<tr>
<td></td>
<td></td>
<td>o Provide targeted and Company-wide training/awareness on antitrust and competition law compliance; target priority audiences</td>
</tr>
</tbody>
</table>