Mapping Ethical Risk

Joint IIA / GACFE Meeting
August 12, 2022

Elizabeth Simon, CPA, CFE, LPEC, CCEP, CIPP-US, SHRM-CP
VP, Compliance
Elizabeth Simon
Vice President, Compliance

My responsibilities:
• Regulatory Compliance
• Business Licensing
• Enterprise Risk Management
• Environmental, Social, Governance Program
• Privacy Program
Agenda

1 Back to the Basics
   • Inherent vs Residual Risk
   • Enterprise Risk Assessments

2 Why is this Important?
   • DOJ Guidance for Compliance Programs

3 Compliance in ERAs
   • Compliance Risk Assessments

4 How to Incorporate Ethics
   • Example assessments

5 What Now?
   • How to take this back and apply it
Inherent Risk vs. Residual Risk
Four Areas of Enterprise Risk

Examples:
- Organizational Structure
- Competitive Risk
- Culture/Ethics
- Reputational Risk
- Customer Priority Shifts
- Succession Planning
- Risk Response Perception
- Geopolitical Risk
- Economic Risk
- Values Misalignment
- Demographic Changes

Examples:
- Spread of Infectious Diseases
- Second Wave of COVID-19
- Customer bankruptcy
- Quality Risk
- Incentives Risk
- Diversity
- Information Technology
- Cybersecurity
- Business Continuity
- Disaster Recovery
- Supply Chain Risk
- Research and Development Risk

Examples:
- Generally Accepted Accounting Principles Compliance
- Fraud
- Capital/Liquidity Risk
- Credit Risk
- Unmanageable Inflation
- Financial Reporting Structure
- Financial Systems
- Transaction Complexity
- Taxation Risk
- Interest Rate Risk
- Restatement Risk

Examples:
- Bribery/corruption
- Third Party Compliance Risk
- Records Management Regulations
- General Regulatory Compliance Risks
- Health and Safety Regulations
- Product Regulations
- Environmental Regulations
- Social Compliance Regulations
- Employment Laws
- Whistleblower Protections
- Intellectual Property
- Legal Liability

When looking at Enterprise Risk, you must look at all risks across the four main categories, and identify where Compliance owns some or all of the risk for the company.
Why is this Important?
The word “risk” is mentioned 53 times in the 2020 DOJ guidance.
“Risk assessment” has its own dedicated section.

“The starting point for a prosecutor’s evaluation of whether a company has a well-designed compliance program is to understand the company’s business from a commercial perspective, how the company has identified, assessed, and defined its risk profile, and the degree to which the program devotes appropriate scrutiny and resources to the spectrum of risks.”
“Risk Assessment” in the 2020 DOJ Guidance

DOJ Guidance

• Justice Manual, “Principles of Federal Prosecution of Business Organizations” (the “Filip Factors”)
  • 8 Factors, including Risk Assessment, Incentives, and Training & Communications
  • Applies specifically to Criminal Anti-Trust, but top officials have indicated they will be considered for all other Criminal Division matters, as well as some or all Civil Division matters.

“If senior management does not actively support and cultivate a culture of compliance, a company will have a paper compliance program, not an effective one.”
Incorporating Compliance into ERM
Enterprise Risk Management Model

- **Likelihood of Occurrence**
  - Low
  - High

- **Impact on the Organization**
  - Low
  - High

- **Compliance Risk**
  - Fraud/Accounting Failure
  - Organizational Structure

- **Reputational Risk**
  - Culture Risk
  - Customer Service/Satisfaction

- **Competitive Environment**
- **Network Takeover**
- **Technology**
Identify the Risks in Your Risk Universe

- **Likelihood of a Violation**
  - Annual Frequency
  - Probability of Occurrence
  - Complexity
  - Business Units Involved
  - Hotline Cases
  - Country Risk
  - Department Risk

- **Impact of a Violation**
  - Financial Loss
  - Fines/Penalties
  - Reputational Impact
  - Employee Morale

- **Velocity of Risk**
  - Level of federal enforcement
  - Fines/penalties against competitors
  - Significant legislation
  - Media spotlight

- **Effectiveness of Controls**
  - Policies/Procedures
  - Training
  - Monitoring
  - Internal Audit Results
  - Management's Response
### Wage and Hour Laws
- Fair Labor Standards Act (FLSA)
- Family and Medical Leave Act (FMLA)
- Consumer Credit Protection Act (CPCA)
- Employee Polygraph Protection Act
- Employee Retirement Income Security Act (ERISA)
- Comprehensive Omnibus Budget Reconciliation Act of 1985 (COBRA)
- Health Insurance Portability and Accountability Act (HIPPA)
- National Labor Relations Act (NLRA)
- Labor-Management Reporting and Disclosure Act (MLRDA) / Landrum-Griffin Act

### Unions
- National Labor Relations Act (NLRA)
- Labor-Management Reporting and Disclosure Act (MLRDA) / Landrum-Griffin Act

### Contract Work Hours and Safety Standards Act
- Davis-Bacon Act
- False Claims Act
- F-A R 52 Compliance
- E-Verify
- Most Favored Nations Clause

### Sherman Act
- Robinson-Patman Act
- Clayton Act
- Truth in Billing

### Data Protection & Privacy
- Gramm Leach Bliley Act
- Payment Card Industry compliance
- Children’s Online Privacy Protection Rule (16 C.F.R. §312)
- Communication Assistance for Law Enforcement Act (CALEA – 18 USC §2510)
- Electronic Communications Privacy Act (18 USC §2701)

### Sales/Marketing Compliance
- Consumer Leasing Act
- CAN-Spam Act
- Truth in Advertising
Gather and Validate Your Data

Identify Risk

Likelihood of a Violation
- Annual Frequency
- Probability of Occurrence
- Complexity
- Business Units Involved
- Hotline Cases
- Country Risk
- Department Risk

Impact of a Violation
- Financial Loss
- Fines/Penalties
- Reputational Impact
- Employee Morale

Velocity of Risk
- Level of federal enforcement
- Fines/penalties against competitors
- Significant legislation
- Media spotlight

Effectiveness of Controls
- Policies/Procedures
- Training
- Monitoring
- Internal Audit Results
- Management's Response

Interview Risk Owner

Continuous Process

Gather Data

Measure Effectiveness

Validate Data
Compliance Risk Heat Map – Inherent Risk
Measure Effectiveness of Your Controls

1. Identify Risk
2. Interview Risk Owner
3. Measure Effectiveness
4. Continuous Process
5. Gather Data
6. Validate Data

- Likelihood of a Violation:
  - Annual Frequency
  - Probability of Occurrence
  - Complexity
  - Business Units Involved
  - Hotline Cases
  - Country Risk
  - Department Risk

- Impact of a Violation:
  - Financial Loss
  - Fines/Penalties
  - Reputational Impact
  - Employee Morale

- Velocity of Risk:
  - Level of federal enforcement
  - Fines/penalties against competitors
  - Significant legislation
  - Media spotlight

- Effectiveness of Controls:
  - Policies/Procedures
  - Training
  - Monitoring
  - Internal Audit Results
  - Management's Response
<table>
<thead>
<tr>
<th>Program Element</th>
<th>Green</th>
<th>Yellow</th>
<th>Red</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oversight</td>
<td>The program has a clear owner that provides reports on a regular basis to the Office of the Chief Compliance Officer</td>
<td>The program has an owner, but does not provide reports to the Office of the Chief Compliance Officer</td>
<td>The program does not have a clear owner</td>
</tr>
<tr>
<td>Due Diligence / Communication</td>
<td>Background check is conducted on all employees’ time of hire in accordance with company’s employment requirements. Relevant employees receive additional screening at time of internal transfer or promotion to confirm background screen and review of existing personnel file and Ethics Line database; review does not indicate that individual hired/promoted has engaged in illegal conduct or other conduct that is inconsistent with an effective compliance program.</td>
<td>Background check is conducted at time of hire but not at time of internal transfer from a non-relevant role to a relevant role or at the time of promotion within relevant roles.</td>
<td>Background checks have not been conducted for all new hires, internal transfers, and promotions, are performed using inconsistent standards between hiring locations, or negative background results are ignored</td>
</tr>
<tr>
<td>Disciplinary Action</td>
<td>The policy clearly states that all employees found to be intentionally non-compliant are disciplined or separated, and all employees found to be unknowingly non-compliant are disciplined or retrained.</td>
<td>The policy is in place, but some employees found to be non-compliant have not been adequately disciplined.</td>
<td>There is no policy in place regarding enforcement and discipline due to non-compliance.</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>Yes. A risk assessment has been completed specifically around this topic area in the past 2 years</td>
<td>Yes. This topic area has been included in a general compliance risk assessment that has been completed in the past 2 years</td>
<td>No. A risk assessment has not been completed in over 2 years</td>
</tr>
<tr>
<td>Auditing</td>
<td>The compliance program has been audited by an independent audit function, such as Internal Audit within the last year</td>
<td>The compliance program has been audited by an independent audit function, such as Internal Audit within the past two years</td>
<td>The compliance program has not been audited by an independent audit function in over two years.</td>
</tr>
<tr>
<td></td>
<td>No non-conformances/issues were detected through audits</td>
<td>Less than 5 minor non-conformances to legal requirements</td>
<td>One or more major non-conformances to legal requirements</td>
</tr>
<tr>
<td>Enforcement Actions</td>
<td>0 investigations/charges per year</td>
<td>1 investigation/charge per year</td>
<td>More than 1 investigation/charge per year</td>
</tr>
<tr>
<td></td>
<td>There are no damages, settlements, or fines from litigation due to compliance failures</td>
<td>Total damages, settlements, and fines from litigation due to compliance failures is within 5% (+ or -) of target</td>
<td>Total damages, settlements, and fines from litigation due to compliance failures is greater than 5% (+ or -) of target</td>
</tr>
<tr>
<td></td>
<td>There are no new lawsuits filed against the company/open litigation matters</td>
<td>Number of new lawsuits filed against the company/open litigation matters is within 5% (+ or -) of target</td>
<td>Number of new lawsuits filed against the company/open litigation matters is greater than 5% (+ or -) of target</td>
</tr>
<tr>
<td>Program Element</td>
<td>Green</td>
<td>Yellow</td>
<td>Red</td>
</tr>
<tr>
<td>--------------------------</td>
<td>-----------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Standards &amp; Procedures</strong></td>
<td>The policy/M&amp;Ps are in place and have been reviewed in the past year</td>
<td>The policy/M&amp;Ps are in place, but have not been reviewed in over a year</td>
<td>No corporate policy/M&amp;Ps exists</td>
</tr>
<tr>
<td></td>
<td>The policy/M&amp;Ps are available to 100% of relevant employees</td>
<td>Greater than 90% of relevant employees have read and understand the policy/M&amp;Ps</td>
<td>The M&amp;Ps are not available to all relevant employees or less than 90% of employees have read and understand the policy</td>
</tr>
<tr>
<td><strong>Training &amp; Education</strong></td>
<td>Trainings are mandatory and available to all relevant employees for understanding all relevant compliance laws</td>
<td>Yes, trainings are available, but are not mandatory and/or are not in a format that will reach all relevant employees</td>
<td>No, trainings are not available</td>
</tr>
<tr>
<td></td>
<td>100% of relevant employees complete the available training courses</td>
<td>Greater than 90% of relevant employees complete the available training courses</td>
<td>Less than 90% of relevant employees complete the available training courses</td>
</tr>
<tr>
<td><strong>Monitoring</strong></td>
<td>There is a process in place to regularly (more than once a year) internally monitor compliance with applicable laws</td>
<td>The compliance program has been internally monitored within the last year</td>
<td>There is no current monitoring being conducted</td>
</tr>
<tr>
<td></td>
<td>No non-conformances/issues were detected through audits</td>
<td>Less than 5 minor non-conformances to legal requirements</td>
<td>One or more major non-conformances to legal requirements</td>
</tr>
<tr>
<td><strong>Corrective Action</strong></td>
<td>The spending level on compliance activities is within budget</td>
<td>The spending level on compliance activities is within 5% (+ or -) of budget</td>
<td>The spending level on compliance activities is greater than 5% (+ or -) of budget</td>
</tr>
<tr>
<td></td>
<td>Less than 90 days</td>
<td>Between 90 and 120 days</td>
<td>Greater than 120 days</td>
</tr>
</tbody>
</table>
# Compliance Summary Scorecard

<table>
<thead>
<tr>
<th>Compliance Area</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>Area Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Labor Relations and Employment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Government Contracts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Antitrust Compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Data Protection and Privacy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sales/Marketing Compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Rating Scale:**

1 - Standards and Procedures
2 - Oversight - Compliance Officer or Compliance Committee
3 - Due Diligence/Open Lines of Communication
4 - Training and Education
5 - Auditing and Monitoring
6 - Enforcement and Disciplinary
7 - Corrective Action Procedures (Response and Prevention)
8 – Risk Assessment
Compliance Risk Heat Map – Residual Risk
Incorporating Ethics into ERM
Analyze the Scope of the Risk

- Identify Risk
- Interview Risk Owner
- Measure Effectiveness
- Continuous Process
- Gather Data
- Validate Data

Likelihood of a Violation:
- Annual Frequency
- Probability of Occurrence
- Complexity
  - Business Units Involved
  - Hotline Cases
  - Country Risk
  - Department Risk

Impact of a Violation:
- Financial Loss
- Fines/Penalties
- Reputational Impact
- Employee Morale

Velocity of Risk:
- Level of federal enforcement
- Fines/penalties against competitors
- Significant legislation
- Media spotlight

Effectiveness of Controls:
- Policies/Procedures
- Training
- Monitoring
- Internal Audit Results
- Management's Response
Ethical Considerations

- Number of alerts generated for policy violations (Travel & Expense; Employee Fraud; Harassment/Discrimination; Bribery, Corruption & Insider Trading; Customer and Vendor Complaints; etc.)
- Number of Hotline complaints
- Training statistics (promptness in taking mandatory training, question-level analysis of success rates, level of participation in non-mandatory training)
- Assess across units (what culture problems do you have and where do you have them)
  - Certain business functions and job categories present a higher level of risk in terms of ethical behavior – Sales; Vendor Management; Trading; etc.
- Focus on level of seniority – Are they leading by example?
Ethical Considerations

• Remote from Manager
• Manage Has Large Span of Control
• Top Performer
• Marginal Performer
• Third Party Selection / Assessment
• Vendor / Counterparty / Due Diligence
• Regulated Activity
• Overseas Market
• High Risk Market
• Signing Authority and Level
• Market Share
• Objectivity required
• Deals with Politically Exposed Persons (PEPs)
Putting it all Together
<table>
<thead>
<tr>
<th>Fraud Risk Level 1</th>
<th>Fraud Risk Level 2</th>
<th>Risk Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cash</td>
<td>Larceny</td>
<td>The risk that an individual in the company steals cash from register</td>
</tr>
<tr>
<td>Fraudulent Disbursements</td>
<td>Billing Scheme</td>
<td>The risk that vendors could be added to the vendor master or modified within the vendor master without a valid reason or approval, causing an increased risk of fraud.</td>
</tr>
<tr>
<td>Billing Scheme</td>
<td>Personal Purchases</td>
<td>Personal purchases with company funds through the A/P system</td>
</tr>
</tbody>
</table>
Risk Description: The risk that an individual in the company steals cash from register.

The risk of Cash Larceny:
- Receive cash daily (5)
- Reasonably possible (3)
- Simple and easy to commit (5)
- Average Likelihood score = 4.3
The risk of Cash Larceny:

- Cash available to employee is limited / small (1)
- Not required to report small thefts (1)
- Limited local media coverage at most if at higher scale (2)
- Isolated morale issues if others know it’s happening, and nothing is done (2)
- Average Impact score = 1.5
Compliance Risk Heat Map – Inherent Risk

The diagram illustrates a matrix where the x-axis represents Likelihood and the y-axis represents Severity. The risk levels are categorized as Low, Medium, and High, with Critical being the highest. The cell at the intersection of Low Likelihood and Low Severity is shaded, indicating a Medium risk level.
### Compliance Risk Assessment Scorecard

<table>
<thead>
<tr>
<th>Program Element</th>
<th>Green</th>
<th>Yellow</th>
<th>Red</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oversight</td>
<td>The program has a clear owner that provides reports on a regular basis to the Office of the Chief Compliance Officer</td>
<td>The program has an owner, but does not provide reports to the Office of the Chief Compliance Officer</td>
<td>The program does not have a clear owner</td>
</tr>
<tr>
<td>Due Diligence / Communication</td>
<td>Background check is conducted on all employees' time of hire in accordance with company's employment requirements. Relevant employees receive additional screening at time of internal transfer or promotion to confirm background screen and review of existing personnel file and Ethics Line database; review does not indicate that individual hired/promoted has engaged in illegal conduct or other conduct that is inconsistent with an effective compliance program.</td>
<td>Background check is conducted at time of hire but not at time of internal transfer from a non-relevant role to a relevant role or at the time of promotion within relevant roles.</td>
<td>Background checks have not been conducted for all new hires, internal transfers, and promotions, are performed using inconsistent standards between hiring locations, or negative background results are ignored</td>
</tr>
<tr>
<td>Disciplinary Action</td>
<td>The policy clearly states that all employees found to be intentionally non-compliant are disciplined or separated, and all employees found to be unknowingly non-compliant are disciplined or retrained.</td>
<td>The policy is in place, but some employees found to be non-compliant have not been adequately disciplined.</td>
<td>There is no policy in place regarding enforcement and discipline due to non-compliance.</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>Yes. A risk assessment has been completed specifically around this topic area in the past 2 years</td>
<td>Yes. This topic area has been included in a general compliance risk assessment that has been completed in the past 2 years</td>
<td>No. A risk assessment has not been completed in over 2 years</td>
</tr>
<tr>
<td>Auditing</td>
<td>The compliance program has been audited by an independent audit function, such as Internal Audit within the last year</td>
<td>The compliance program has been audited by an independent audit function, such as Internal Audit within the past two years</td>
<td>The compliance program has not been audited by an independent audit function in over two years.</td>
</tr>
<tr>
<td></td>
<td>No non-conformances/issues were detected through audits</td>
<td>Less than 5 minor non-conformances to legal requirements</td>
<td>One or more major non-conformances to legal requirements</td>
</tr>
<tr>
<td>Enforcement Actions</td>
<td>0 investigations/charges per year</td>
<td>1 investigation/charge per year</td>
<td>More than 1 investigation/charge per year</td>
</tr>
<tr>
<td></td>
<td>There are no damages, settlements, or fines from litigation due to compliance failures</td>
<td>Total damages, settlements, and fines from litigation due to compliance failures is within 5% (+ or -) of target</td>
<td>Total damages, settlements, and fines from litigation due to compliance failures is greater than 5% (+ or -) of target</td>
</tr>
<tr>
<td></td>
<td>There are no new lawsuits filed against the company/open litigation matters</td>
<td>Number of new lawsuits filed against the company/open litigation matters is within 5% (+ or -) of target</td>
<td>Number of new lawsuits filed against the company/open litigation matters is greater than 5% (+ or -) of target</td>
</tr>
<tr>
<td>Program Element</td>
<td>Green</td>
<td>Yellow</td>
<td>Red</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Standards &amp; Procedures</td>
<td>The policy/M&amp;Ps are in place and have been reviewed in the past year</td>
<td>The policy/M&amp;Ps are in place, but have not been reviewed in over a year</td>
<td>No corporate policy/M&amp;Ps exists</td>
</tr>
<tr>
<td></td>
<td>The policy/M&amp;Ps are available to 100% of relevant employees</td>
<td>Greater than 90% of relevant employees have read and understand the policy/M&amp;Ps</td>
<td>The M&amp;Ps are not available to all relevant employees or less than 90% of employees have read and understand the policy</td>
</tr>
<tr>
<td>Training &amp; Education</td>
<td>Trainings are mandatory and available to all relevant employees for understanding all relevant compliance laws</td>
<td>Yes, trainings are available, but are not mandatory and/or are not in a format that will reach all relevant employees</td>
<td>No, trainings are not available</td>
</tr>
<tr>
<td></td>
<td>100% of relevant employees complete the available training courses</td>
<td>Greater than 90% of relevant employees complete the available training courses</td>
<td>Less than 90% of relevant employees complete the available training courses</td>
</tr>
<tr>
<td>Monitoring</td>
<td>There is a process in place to regularly (more than once a year) internally monitor compliance with applicable laws</td>
<td>The compliance program has been internally monitored within the last year</td>
<td>There is no current monitoring being conducted</td>
</tr>
<tr>
<td></td>
<td>No non-conformances/issues were detected through audits</td>
<td>Less than 5 minor non-conformances to legal requirements</td>
<td>One or more major non-conformances to legal requirements</td>
</tr>
<tr>
<td>Corrective Action</td>
<td>The spending level on compliance activities is within budget</td>
<td>The spending level on compliance activities is within 5% (+ or -) of budget</td>
<td>The spending level on compliance activities is greater than 5% (+ or -) of budget</td>
</tr>
<tr>
<td></td>
<td>Less than 90 days</td>
<td>Between 90 and 120 days</td>
<td>Greater than 120 days</td>
</tr>
</tbody>
</table>
## Compliance Summary Scorecard

<table>
<thead>
<tr>
<th>Compliance Area</th>
<th>Program Element</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>Area Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud - Larceny</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2.68</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Rating Scale:**

1 - Standards and Procedures
2 - Oversight - Compliance Officer or Compliance Committee
3 - Due Diligence/Open Lines of Communication
4 - Training and Education
5 - Auditing and Monitoring
6 - Enforcement and Disciplinary
7 - Corrective Action Procedures (Response and Prevention)
8 – Risk Assessment
Compliance Risk Heat Map – Inherent Risk

<table>
<thead>
<tr>
<th>Severity</th>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>High</td>
<td>Critical</td>
</tr>
</tbody>
</table>

- Low likelihood and low severity results in Medium risk.
- High likelihood and high severity results in Critical risk.
Ethical Considerations

- Remote from Manager
- Manage Has Large Span of Control
- Top Performer
- ✓ Marginal Performer
- Third Party Selection / Assessment
- Vendor / Counterparty / Due Diligence
- Regulated Activity
- Overseas Market
- High Risk Market
- Signing Authority and Level
- Market Share
- Objectivity required
- Deals with Politically Exposed Persons (PEPs)
Ethical Considerations

• Number of alerts generated for policy violations (Travel & Expense; Employee Fraud; Harassment/Discrimination; Bribery, Corruption & Insider Trading; Customer and Vendor Complaints; etc.)

✓ Number of Hotline complaints

✓ Training statistics (promptness in taking mandatory training, question-level analysis of success rates, level of participation in non-mandatory training)

✓ Assess across units (what culture problems do you have and where do you have them)
  • Certain business functions and job categories present a higher level of risk in terms of ethical behavior – Sales; Vendor Management; Trading; etc.
  • Focus on level of seniority – Are they leading by example?
• Review/count of register each evening
• Monthly trend report for missing money
• Security cameras in stores
• Second person makes deposits
• Money kept in safe after register is counted

• Insurance Policy for Employee Fraud

Reduce Likelihood for effective controls.

Reduce Impact for effective control.
Enterprise Risk Management Model

![Diagram showing various risk factors and their likelihood of occurrence and impact on the organization.]

- **Likelihood of Occurrence**
  - High
  - Low

- **Impact on the Organization**
  - High
  - Low

- **Risk Factors**
  - Fraud/Accounting Failure
  - Network Takeover
  - Competitive Environment
  - Reputational Risk
  - Technology
  - Customer Service/Satisfaction
  - Culture Risk
  - Organizational Structure
  - Compliance Risk

The diagram illustrates the enterprise risk management model with various risk factors plotted on a 2x2 matrix based on their likelihood of occurrence and impact on the organization.
<table>
<thead>
<tr>
<th>Risk Level 1</th>
<th>Risk Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cybersecurity / Information Security Breach</td>
<td>The risk that the company's information technology does not have adequate controls and allows for threats such as hacking, data breaches, security incidents, etc.</td>
</tr>
<tr>
<td>Privacy Regulations</td>
<td>The risk of the company not adhering to the regulations applicable to the company</td>
</tr>
<tr>
<td>Receipt and Handling of PII</td>
<td>The risk that the company does not properly handle resident, vendor, or team member PII, resulting in a loss or breach of the data.</td>
</tr>
<tr>
<td>Data Governance</td>
<td>The risk that the company does not have the proper governance (availability, usability, and security) of the data in its enterprise systems to ensure that data is consistent, trustworthy and not misused.</td>
</tr>
</tbody>
</table>
Assess the Likelihood

Risk Description: The risk that the company's information technology does not have adequate controls and allows for threats such as hacking, data breaches, security incidents, etc.

The risk of Cybersecurity / Information Security Breaches

- Use systems daily / receive threats daily (5)
- Almost certain (5)
- Mostly understandable and able to commit (4)

- Average Likelihood score = 4.7
Assess the Impact

The risk of Cybersecurity / Information Security Breaches.

- Huge financial loss if systems down or if theft of information (5)
- Data breach requirements by state (5)
- If major breach, could impact media coverage, depending on response (4)
- Could result in general employee morale issues and questions about company continuity (3)

- Average Impact score = 4.3
Compliance Risk Heat Map – Inherent Risk
<table>
<thead>
<tr>
<th>Program Element</th>
<th>Green</th>
<th>Yellow</th>
<th>Red</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Oversight</strong></td>
<td>The program has a clear owner that provides reports on a regular basis to the Office of the Chief Compliance Officer</td>
<td>The program has an owner, but does not provide reports to the Office of the Chief Compliance Officer</td>
<td>The program does not have a clear owner</td>
</tr>
<tr>
<td><strong>Due Diligence / Communication</strong></td>
<td>Background check is conducted on all employees' time of hire in accordance with company's employment requirements. Relevant employees receive additional screening at time of internal transfer or promotion to confirm background screen and review of existing personnel file and Ethics Line database; review does not indicate that individual hired/promoted has engaged in illegal conduct or other conduct that is inconsistent with an effective compliance program.</td>
<td>Background check is conducted at time of hire but not at time of internal transfer from a non-relevant role to a relevant role or at the time of promotion within relevant roles.</td>
<td>Background checks have not been conducted for all new hires, internal transfers, and promotions, are performed using inconsistent standards between hiring locations, or negative background results are ignored</td>
</tr>
<tr>
<td><strong>Disciplinary Action</strong></td>
<td>The policy clearly states that all employees found to be intentionally non-compliant are disciplined or separated, and all employees found to be unknowingly non-compliant are disciplined or retrained.</td>
<td>The policy is in place, but some employees found to be non-compliant have not been adequately disciplined.</td>
<td>There is no policy in place regarding enforcement and discipline due to non-compliance.</td>
</tr>
<tr>
<td><strong>Risk Assessment</strong></td>
<td>Yes. A risk assessment has been completed specifically around this topic area in the past 2 years</td>
<td>Yes. This topic area has been included in a general compliance risk assessment that has been completed in the past 2 years</td>
<td>No. A risk assessment has not been completed in over 2 years</td>
</tr>
<tr>
<td><strong>Auditing</strong></td>
<td>The compliance program has been audited by an independent audit function, such as Internal Audit within the last year</td>
<td>The compliance program has been audited by an independent audit function, such as Internal Audit within the past two years</td>
<td>The compliance program has not been audited by an independent audit function in over two years.</td>
</tr>
<tr>
<td><strong>Enforcement Actions</strong></td>
<td>0 investigations/charges per year</td>
<td>1 investigation/charge per year</td>
<td>More than 1 investigation/charge per year</td>
</tr>
<tr>
<td></td>
<td>There are no damages, settlements, or fines from litigation due to compliance failures</td>
<td>Total damages, settlements, and fines from litigation due to compliance failures is within 5% (+ or -) of target</td>
<td>Total damages, settlements, and fines from litigation due to compliance failures is greater than 5% (+ or -) of target</td>
</tr>
<tr>
<td></td>
<td>There are no new lawsuits filed against the company/open litigation matters</td>
<td>Number of new lawsuits filed against the company/open litigation matters is within 5% (+ or -) of target</td>
<td>Number of new lawsuits filed against the company/open litigation matters is greater than 5% (+ or -) of target</td>
</tr>
<tr>
<td>Program Element</td>
<td>Green</td>
<td>Yellow</td>
<td>Red</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Standards &amp; Procedures</strong></td>
<td>The policy/M&amp;Ps are in place and have been reviewed in the past year</td>
<td>The policy/M&amp;Ps are in place, but have not been reviewed in over a year</td>
<td>No corporate policy/M&amp;Ps exists</td>
</tr>
<tr>
<td></td>
<td>The policy/M&amp;Ps are available to 100% of relevant employees</td>
<td>Greater than 90% of relevant employees have read and understand the policy/M&amp;Ps</td>
<td>The M&amp;Ps are not available to all relevant employees or less than 90% of employees have read and understand the policy</td>
</tr>
<tr>
<td><strong>Training &amp; Education</strong></td>
<td>Trainings are mandatory and available to all relevant employees for understanding all relevant compliance laws</td>
<td>Yes, trainings are available, but are not mandatory and/or are not in a format that will reach all relevant employees</td>
<td>No, trainings are not available</td>
</tr>
<tr>
<td></td>
<td>100% of relevant employees complete the available training courses</td>
<td>Greater than 90% of relevant employees complete the available training courses</td>
<td>Less than 90% of relevant employees complete the available training courses</td>
</tr>
<tr>
<td><strong>Monitoring</strong></td>
<td>There is a process in place to regularly (more than once a year) internally monitor compliance with applicable laws</td>
<td>The compliance program has been internally monitored within the last year</td>
<td>There is no current monitoring being conducted</td>
</tr>
<tr>
<td></td>
<td>No non-conformances/issues were detected through audits</td>
<td>Less than 5 minor non-conformances to legal requirements</td>
<td>One or more major non-conformances to legal requirements</td>
</tr>
<tr>
<td><strong>Corrective Action</strong></td>
<td>The spending level on compliance activities is within budget</td>
<td>The spending level on compliance activities is within 5% (+ or -) of budget</td>
<td>The spending level on compliance activities is greater than 5% (+ or -) of budget</td>
</tr>
<tr>
<td></td>
<td>Less than 90 days</td>
<td>Between 90 and 120 days</td>
<td>Greater than 120 days</td>
</tr>
</tbody>
</table>
### Compliance Summary Scorecard

<table>
<thead>
<tr>
<th>Compliance Area</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>Area Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fraud - Larceny</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2.81</td>
</tr>
<tr>
<td>Standards and Procedures</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oversight</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance Officer or Compliance Committee</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Due Diligence/Open Lines of Communication</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training and Education</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Auditing and Monitoring</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enforcement and Disciplinary</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Corrective Action Procedures (Response and Prevention)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Risk Assessment</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Rating Scale:**

1 - Standards and Procedures
2 - Oversight - Compliance Officer or Compliance Committee
3 - Due Diligence/Open Lines of Communication
4 - Training and Education
5 - Auditing and Monitoring
6 - Enforcement and Disciplinary
7 - Corrective Action Procedures (Response and Prevention)
8 – Risk Assessment
Compliance Risk Heat Map – Inherent Risk
Ethical Considerations

✓ Remote from Manager
  • Manage Has Large Span of Control
  • Top Performer
  • Marginal Performer
✓ Third Party Selection / Assessment
✓ Vendor / Counterparty / Due Diligence
  • Regulated Activity
✓ Overseas Market
  • High Risk Market
  • Signing Authority and Level
  • Market Share
  • Objectivity required
  • Deals with Politically Exposed Persons (PEPs)
Ethical Considerations

• Number of alerts generated for policy violations (Travel & Expense; Employee Fraud; Harassment/Discrimination; Bribery, Corruption & Insider Trading; Customer and Vendor Complaints; etc.)

• Number of Hotline complaints

✓ Training statistics (promptness in taking mandatory training, question-level analysis of success rates, level of participation in non-mandatory training)

• Assess across units (what culture problems do you have and where do you have them)
  • Certain business functions and job categories present a higher level of risk in terms of ethical behavior – Sales; Vendor Management; Trading; etc.

• Focus on level of seniority – Are they leading by example?
Compliance Risk Heat Map – Inherent Risk

- **Severity**
  - Low
  - Medium
  - High

- **Likelihood**
  - Low
  - Medium
  - High

- Inherent Risk: High
Other Controls

- Penetration testing
- Review of access controls
- Vendor security reviews at onboarding
- Reduction of number of admin accounts

- Cyber Insurance policy

Reduce Likelihood for effective controls.

Reduce Impact for effective control.
Compliance Risk Heat Map – Residual Risk

- **Severity**
  - Low
  - Medium
  - High

- **Likelihood**
  - Low
  - Medium
  - High

- **Critical**
- **High**
- **Medium**
- **Low**
So What? Now What?
Manage/Treat the Risk

- Transfer / Insure
- Avoid / Mitigate
- Accept / Monitor
- Reduce / Mitigate

Impact / Severity

Likelihood
• Proper Enterprise Risk Assessments, which incorporate compliance and ethics, can lead to identification of areas where management should spend the most resources.

• Hotline reporting rates increase when the company has:
  • An effective compliance program
  • A strong ethical culture
  • Both top and middle management that are committed to ethics
  • The same standard for misconduct by all levels of employees in the company
  • Only isolated incidents of misconduct instead of pervasive, company-wide misconduct

An Ethical Culture Leads Employees to Do the Right Thing
Questions?

ELIZABETH SIMON
VP, COMPLIANCE
FIRSTKEY HOMES