The One Page Compliance Program

“Simplicity means the achievement of maximum effect with minimum means.”—Albert Einstein

“I would not give a fig for the simplicity this side of complexity, but I would give my life for the simplicity on the other side of complexity.”—Oliver Wendell Holmes

Introductions

- Deena King
  - Managing Director
  - Pure Knowledge Consulting
  - 30 Year Cross-trained Professional
  - 9 years Audit/Compliance
- Specialties
  - Compliance Program Design
  - Compliance Program Evaluation
  - Continuous Improvement
- Industries:
  - Higher Education
  - Utility
Agenda

• Compliance as a Business Process
  – Core Process Components
  – Risks and Value-added
• Compliance Program Design
  – The One Page Compliance Program
    • “Indexing”
• Review

Compliance as a Business Process

What we can learn from “best practice” frameworks
Compliance as a Business Process

- The “7 Elements” from the FSG
- “Best Practice” Frameworks
  - COSO “Cube”
    - Sarbanes-Oxley Controls
  - COBIT
    - Technology Compliance
    - Process Controls
  - OCEG “Red Book”
    - Open Compliance and Ethics Group
  - Continuous Improvement Models
    - Deming’s “Plan, Do, Check, Act”
The organization shall periodically assess the risk of criminal conduct and shall take appropriate steps to design, implement, or modify each requirement (§§ 8B2.1.c). Delivered: Annual/Quarterly Risk Assessments; Compliance Requirements

Deliverables:  Annual/Quarterly Risk Assessments; Compliance Requirements

The organization shall establish standards and procedures to prevent and detect criminal conduct (§§ 8B2.1.b.1). Delivered: Documentation

Deliverables:  Documentation

The organization’s compliance and ethics program shall be reasonably implemented, promoted and enforced consistently throughout the organization (§§ 8B2.1.a.2 & b.6). Delivered: An Implemented Program

Deliverables:  An Implemented Program

Establish/Modify Compliance Organization

Governing authority shall be knowledgeable and exercise reasonable oversight; High-level personnel shall ensure the organization has an effective compliance program; Specific individuals shall be delegated day-to-day operational responsibility; Exercise due diligence (§§ 8B2.1.b.2.A-C & 3). Delivered: Org Chart; Job Descriptions; Background Checks

Deliverables:  Org Chart; Job Descriptions; Background Checks

Leadership/ Corporate Culture

Promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law (§ 8B2.1.a.2 and b)

Deliverables:  Audit Program; Program Evaluation; Hotline

Monitor, Audit, and Report

Monitoring and auditing to detect criminal conduct; Periodically evaluate the effectiveness of the organization’s compliance program; Publicize a reporting system (§ 8B2.1.b.2.A-C). Delivered: Audit Program; Program Evaluation; Hotline

Deliverables:  Audit Program; Program Evaluation; Hotline

Communicate Standards, Policies, and Procedures

Communicate periodically standards and procedures, and other aspects to employees by conducting effective training programs and otherwise disseminating information (§§ 8B2.1.b.4). Delivered: Communication and Training Plans

Deliverables: Communication and Training Plans

Implement, Promote and Enforce

The organization’s compliance and ethics program shall be reasonably implemented, promoted and enforced consistently throughout the organization (§§ 8B2.1.a.2 & b.6). Delivered: An Implemented Program

Deliverables:  An Implemented Program

The “7 Elements” from the Federal Sentencing Guidelines

• Standards and Procedures
• High-level Oversight
• Screening
• Training and Education
• Monitoring, Auditing, and Reporting
• Promotion and Enforcement
• Response and Correction
Utility Industry Example

- Federal Energy Regulatory Commission (FERC)
  - Policy Statement on Compliance
  - Policy Statement on Enforcement
- North American Electric Reliability Corporation (NERC)
The Compliance Process and the FERC Policy Statement on Compliance

<table>
<thead>
<tr>
<th>Leadership/Corporate Culture</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsibility for a culture of compliance rests squarely on the shoulders of senior management (see paragraphs 1 and 13)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Continuous Improvement</th>
</tr>
</thead>
<tbody>
<tr>
<td>The question of whether new or modified prospective controls are needed to prevent a recurrence (see paragraph 21)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Assess Risk/Identify Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Each company has to determine the optimum investment to make in compliance measures in light of its resources and risks (see paragraph 17)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Establish/Modify Compliance Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>The best program will not succeed unless senior management actively embraces the importance of compliance; Senior management may designate...compliance officials within the company (see paragraphs 13 and 15)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Document Standards, Policies, and Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Companies should invest in systematic preventative measures (see paragraph 16)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Communicate Standards, Policies, and Procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>Senior management should communicate its commitment to compliance frequently; Systematic and effective preventative measures such as...training are fundamental (see paragraphs 14 and 16)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Implement, Promote and Enforce</th>
</tr>
</thead>
<tbody>
<tr>
<td>The company must...implement the program; companies should expeditiously put an end to wrongful conduct and report it promptly; correct the problem; remediate the misconduct (see paragraphs 16, 19, and 21)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Monitor, Audit, and Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Effective accountability for compliance; periodic review and evaluation of the effectiveness of the compliance program; detect violations; systematic internal auditing and self-reporting (see paragraphs 16, 18-20)</td>
</tr>
</tbody>
</table>

*FERC Compliance with Statutes, Regulations, and Orders, Docket No. PL09-1-000, October 2008.

Questions? Comments?
Value and Risk

- Risk Assessment/Identify Requirements
- Establish/Modify Organizational Structure
- Document Standards, Policies, and Procedures
- Communicate Standards, Policies, and Procedures
- Implement, Promote, and Enforce
- Monitor, Audit, and Report
- Leadership/Corporate Culture

Compliance Program Design

The One Page Compliance Program
The One Page Compliance Program

- Summary of the Compliance Process
  - How will we:
    - Assess Risk/Identify Requirements?
    - Establish/Modify our Compliance Organization?
    - Document our Standards, Policies, and Procedures?
    - Communicate our Standards, Policies, and Procedures?
    - Implement, Promote, and Enforce?
    - Monitor, Audit, and Report?
    - Continuously Improve?
    - Lead?

Using the Compliance Process
To Design/Enhance Compliance Programs

<table>
<thead>
<tr>
<th>Assess Risk/Identify Requirements</th>
<th>Leadership/Corporate Culture</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deliverables:</td>
<td>Deliverables:</td>
</tr>
<tr>
<td>- Annual/Quarterly Risk Assessments</td>
<td>- Leadership</td>
</tr>
<tr>
<td>- Compliance Requirements</td>
<td></td>
</tr>
<tr>
<td>Establish/Modify Compliance Organization</td>
<td></td>
</tr>
<tr>
<td>Deliverables:</td>
<td></td>
</tr>
<tr>
<td>- Org Chart</td>
<td></td>
</tr>
<tr>
<td>- Job Descriptions</td>
<td></td>
</tr>
<tr>
<td>- Background Checks</td>
<td></td>
</tr>
<tr>
<td>Document Standards, Policies, and Procedures</td>
<td></td>
</tr>
<tr>
<td>Deliverables:</td>
<td></td>
</tr>
<tr>
<td>- Documentation</td>
<td></td>
</tr>
<tr>
<td>Communicate Standards, Policies, and Procedures</td>
<td></td>
</tr>
<tr>
<td>Deliverables:</td>
<td></td>
</tr>
<tr>
<td>- Communication</td>
<td></td>
</tr>
<tr>
<td>- Training Plans</td>
<td></td>
</tr>
<tr>
<td>Implement, Promote and Enforce</td>
<td>Continuous Improvement</td>
</tr>
<tr>
<td>Deliverables:</td>
<td>Deliverables:</td>
</tr>
<tr>
<td>- An Implemented Program</td>
<td>- Enforcement</td>
</tr>
<tr>
<td>Monitor, Audit, and Report</td>
<td>- Modifications to any or all noted deliverables</td>
</tr>
</tbody>
</table>
The One Page Compliance Program

Our Compliance Program

I. Risk Assessment/Identify Requirements:
   - Risk Assessment
   - Compliance Requirements

II. Establish/Modify Organizational Structure:
   - Key Chain:
   - Roles/Responsibilities:
   - Background Checks:

III. Document Standards, Policies, and Procedures:
   - Documentation:

IV. Communicate Standards, Policies, and Procedures:
   - Communication Plan:
   - Training Plan:

V. Implement, Process, and Evaluate:
   - Implementation Strategy and Records:

VI. Monitor, Audit, and Report:
   - Audit Program:
   - Compliance Program Evaluations:
   - Retain:

The One Page Compliance Program: Web Example

The Pure Knowledge Consulting Compliance Program is based on the model outlined by the Federal Sectoric Guidelines (FSG). The program document can be found here [FSG Link]. The deliverables from the program can be found by following the links below.

I. Risk Assessment/Identify Requirements:
   - FSG Compliance Risk Assessments (Annual & Quarterly Updates)
   - FSG Compliance/Compliance Requirements

II. Establish/Modify Organizational Structure:
   - FSG Compliance Key Chain:
   - FSG Compliance/Compliance Policies and Responsibilities
   - FSG Background Checks Policy and Procedures

III. Document Standards, Policies, and Procedures:
   - FSG Compliance/Compliance Policies and Procedures

IV. Communicate Standards, Policies, and Procedures:
   - FSG Compliance/Compliance Plans
   - FSG Compliance Tracking Plan
   - FSG Compliance Training Plan
   - FSG Compliance/Compliance Records

V. Implement, Process, and Evaluate:
   - FSG Compliance/Compliance Evaluations

VI. Monitor, Audit, and Report:
   - FSG Audit/Compliance
   - FSG Compliance/Compliance Program Evaluation
   - FSG Compliance/Compliance Program Evaluation Reports

© 2010 Pure Knowledge Consulting, LLC
The One Page Compliance Program: Paper Example

Flexible and Adaptable

- One Page “Index”:
  - Corporate Executive Summary
  - Regulation Specific
    - FERC
    - EEO
    - Sarbanes-Oxley
  - Division/Department-level
    - HR
    - Safety
The Compliance Process:
Organizational Structure

Governance
Risk: Organization-wide
Org: Board; Senior Management*
Document and Communicate: Corporate Compliance Program; Policy
Promote and Enforce: Policy
Monitor: Policy; Effectiveness of Program

Management
Risk: Mid-level
Org: Management
Document and Communicate: Departmental Compliance Programs; Policies and Procedures
Promote and Enforce: Departmental Policies and Procedures
Monitor: Effectiveness of departmental programs; Departmental Policies and Procedures

Performance/Operational
Risk: Operational
Org: Front-line Professionals
Document and Communicate: Operational Procedures
Promote and Enforce: Operational Procedures
Monitor: Operational Procedures

*Companies subject to the FERC Standards of Conduct must designate a Chief Compliance Officer

Case Study Examples
Questions? Comments?
Appendix A

Additional Information on “Best Practice” Frameworks

COSO Management Controls

• At Multiple levels across multiple functions:
  – Internal Environment
  – Objective Setting
  – Event Identification
  – Risk Assessment
  – Risk Response
  – Control Activities
  – Communication
  – Monitoring
COBIT “Process Controls”

OCEG Foundation-level Guidelines

- Culture
  - Ethics
  - Risk
  - Governance
  - Workforce

- Organization/Personnel
  - Leadership
  - Oversight
  - Strategy
  - Operations

- Process
  - Plan/Organize
  - Prevent/Protect/Prepare
  - Monitor/Evaluate
  - Respond/Improve

- Technology
Assess Risk/ Identify Requirements

Establish/Modify Compliance Organization

Document Standards, Policies, and Procedures

Communicate Standards, Policies, and Procedures

Implement, Promote and Enforce

Monitor, Audit, and Report

Leadership/ Corporate Culture

© 2010

Promote an organizational culture that encourages ethical conduct and a commitment to compliance with the law (§ 8B2.1.a.2 and b)

Continuous Improvement

• Objective Setting
• Risk Assessment

• Risk Response
• Communication

• Entity-level; Division,
• Business Unit; Subdivision

• Internal Environment
• Strategic; Operations
• Compliance

• Control Activities

Leadership/ Corporate Culture

• Goals and Objectives
• Performance Improvement

• Ownership

• Compare Measurements (Performance Improvement)

• High-level Oversight

• Repeatability
• Define Policies, Plans, Procedures

• Performance Metrics (Performance Improvement)

• Roles and Responsibilities
• Communicate Policies, Plans

• Monitoring
• Reporting

© 2010

Pure Knowledge Consulting LLC
Compliance as a Process: Map to OCEG Foundation

- **Assess Risk/Identify Requirements**
  - Culture: Risk
  - Leadership: Strategy
  - Process: Respond, Improve

- **Establish/Modify Compliance Organization**
  - Leadership: Oversight, Operations

- **Document Standards, Policies, and Procedures**
  - Culture: Ethics, Governance, Workforce
  - Organization: Leadership
  - Process: Plan, Organize

- **Communicate Standards, Policies, and Procedures**
  - Process: Prepare

- **Implement, Promote and Enforce**
  - Process: Prevent, Protect

- **Monitor, Audit, and Report**
  - Process: Monitor, Evaluate

---

The Compliance Process and the FERC Policy Statement on Enforcement*

- **Risk Assessment**
  - An inventory of current compliance risks (see paragraph 59)

- **Establish/Modify Compliance Organization**
  - An independent Compliance Officer or other high-ranking official who reports to the Chief Executive Officer, the Board, or a committee; Tie regulatory compliance to personnel assessments and compensation, including compensation of management (see paragraphs 58 and 59)

- **Document Standards, Policies, and Procedures**
  - An established, formal, well documented program for internal compliance; an inventory of current compliance practices (see paragraphs 58 and 59)

- **Communicate Standards, Policies, and Procedures**
  - Training on rules and regulations that is sufficiently detailed and thorough is provided to all relevant employees; frequent mandatory training programs that include “real world” examples (see paragraphs 58 and 59)

- **Promotion and Enforcement**
  - There are identifiable, measurable performance targets; there are disciplinary consequences in place for infractions of Commission requirements; the company looks for repeat offenses (see paragraph 59)

- **Monitor, Audit, and Report**

---

**Leadership/Corporate Culture**

- Compliance is fully supported by senior management and they are actively involved in compliance efforts; company policies on compensation and promotion take into consideration employee compliance; sufficient funding is provided for the administration of compliance programs (see paragraphs 58 and 59)

**Continuous Improvement**

- The company frequently modifies the compliance program; the company implements more effective internal controls and procedures to prevent recurrence of misconduct (see paragraph 58)

---

*FERC Enforcement of Statutes, Regulations, and Orders, Docket No. PL08-3-000, May 2008.