Conducting Compliance Risk Assessments: Understanding Risk at the Functional Level

Sonal J. Shah, CPA, MSPA, CHC, CGMA
Chief Ethics and Compliance Officer
Stanford University

Career - Responsibilities
- Compliance and Ethics,
- Conflict of Interest,
- Risk, Enterprise Risk Management,
- Investigations,
- Privacy, and
- Internal Audit, Financial Analysis, …

Career - Profile
- Public Accounting Firms
- Aetna
- Yale New Haven Health System
- Landmark Medical Center
Career - Profile

- Tufts Medical Center
- Hartford HealthCare
- Harvard University
  - School of Dental Medicine
- Stanford University

Disclaimer
(To prevent any misunderstanding)

- My Individual View.
- And, not that of Stanford University, or any of my Previous Employers.

Compliance Programs
By a Show of Hands…

How many would say that they have
• an “Evolving” Compliance Program vs.
• a “Mature” Compliance Program?

How about
• A Structured/formal Enterprise Risk Management Program?

Stanford University’s Program

Stanford University – Not-for-Profit World – Stakeholders

- Students
  - Education and Learning
- Governmental and Private Sponsors
  - Research
- Donors
  - Various Causes and Activities
- Patients and Insurers
  - Patient Care
Promote - Compliance and Ethics

- Strive to Ensure:
  - Funds Entrusted are Used Responsibly and for their Intended Purpose.
  - Activities are Conducted for the Intended Purpose.


Seven Elements of an Effective Compliance Program

- Federal Sentencing Guidelines
  - The Seven Elements
  - “Best Business Practices”

- Review, Reveal, Rectify

Seven Elements of an Effective Compliance Program

1. Standards and Procedures.
2. Governance, Organization and Reporting.
3. Efforts to Include only Personnel consistent with an Effective Compliance and Ethics Program.
4. Training and Education.
5. Program Monitoring and Auditing, Evaluation of Program Effectiveness.
6. Performance Incentives, Consistent Enforcement/Appropriate Discipline.
7. Responding to Non-compliance and Modifying the Program as Necessary.
Risk Assessments in Higher Education

- Internal Audit – Annual Risk Assessments.
- Enterprise Risk Assessment.
- Compliance Risk Assessments.

Compliance Risk - Definition

Compliance risk is the threat posed to an organization’s financial, organizational, or reputational standing resulting from violations of laws, regulations, codes of conduct, or organizational standards of practice.

Source: Deloitte - Compliance risk assessments: The third ingredient in a world-class ethics and compliance program (2015).

Understanding Compliance Risk

Create a Structure so as to proactively:
- Identify Compliance Risks,
- Assess Compliance Risks,
- Manage Compliance Risks, and finally
- Monitor Compliance Risks.

Purpose: To ensure that Risk is mitigated or reduced to a level that is acceptable to Sr. Management. Exposure is Reduced!
Compliance Risk Management

Concept – Important!
Risk is mitigated or reduced to a level that is acceptable to Senior Management.

- Risk Tolerance
- Threshold

Compliance Risk Management - In Functional Areas

Create a Compliance Matrix = Universe of Compliance Risk.

- With Name of Area.
- Establish Accountability:
  - Cabinet/Sr. Management Risk Owner.
  - Office/Role - who ensures compliance within the Functional Area.

Design a Process for Gathering Information
Then, Produce a “Report”

Two Tools
1. Data Collection Form
2. Compliance Risk Assessment

In Both, Functional Area Assessed against:
• the Seven Elements of an Effective Compliance Program.

However, Use and Frequency Differ.
### Data Collection Form - 1

**A. RULES, REGULATIONS, AND OTHER REGULATORY REQUIREMENTS**

i. Please list all relevant federal laws/regulations that apply to your compliance area, if any.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

i. Please list all relevant state laws/regulations that apply to your compliance area, if any.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

i. Please list all relevant local laws/regulations that apply to your compliance area, if any.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

i. Please list all other sources for guidance/best practices (e.g., professional organizations, journal subscriptions, listservs, etc.), if any.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Data Collection Form - 2

**B. REGULATORY CHANGES, NEW DEVELOPMENTS, EMERGING COMPLIANCE ISSUES, AND GOVERNMENTAL ENFORCEMENT ACTIVITY**

i. Please describe the regulatory changes in your area, if any.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

i. Please describe the new developments, and/or emerging compliance issues in your area, if any.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

i. Please describe knowledge of governmental enforcement activity in your area, if any.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Data Collection Form – 3

**SEVEN ELEMENTS OF AN EFFECTIVE COMPLIANCE AND ETHICS PROGRAM**

The seven elements are set out in the Federal Sentencing Guidelines (FSG) for organizations. Although these elements have their origins in U.S. criminal law, they are recognized as the appropriate standard for evaluating the effectiveness of a compliance and ethics program. In 2010, the Federal Sentencing Guidelines were amended to include titles and emphasized promoting an ethical business culture, beyond simply compliance with laws.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**1. STANDARDS AND PROCEDURES**

i. Please provide hyperlinks or attachments to all relevant Policies and Procedures (P&P) in your compliance area. Are several P&P exist? Is there one hyperlink that provides access to all relevant P&P?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

ii. Have P&P been updated to reflect regulatory changes, new developments, and/or emerging compliance issues? If so, how?

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Data Collection Form – 4

A. GOVERNANCE

1. What kind of reporting is performed for your compliance area? If any, please include the frequency of the reporting.

2. What is it reported to? (e.g. Senior Management, Committees, Board, etc.)?

3. Are there any committees that meet to review, oversee, provide guidance to your compliance area? If so, please include the number of members and frequency of committee meetings.

Data Collection Form – 5

ORGANIZATIONAL STRUCTURE

1. Please describe the reporting structure and/or attach a current organization chart of your compliance area.

REPORTING

2. Describe the metrics for compliance activities in your area (e.g. staffing, transactions, volume, issues identified, reports issued, dollars involved, etc.).

3. Any reporting to federal/state/local agencies required by law? If so, what are the requirements for reporting?

Data Collection Form – 6

PERSONNEL

1. Beyond the criminal, background and reference checks that Stanford conducts on all new staff, does your compliance area require additional background checks or verification of personnel? If so, please explain.

2. How are risk owners and staff in your compliance area appropriately trained to fulfill their responsibilities and stay current with regulatory requirements (e.g. maintaining professional certifications, attending educational conferences, training, etc.)?
### Data Collection Form – 7

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1. Training and Education for Stanford Community</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>What training does your compliance area provide on regulatory requirements and/or P&amp;P?</td>
</tr>
<tr>
<td></td>
<td>What is the training format (e.g., live, web-based, etc.)?</td>
</tr>
<tr>
<td></td>
<td>To whom and how often is training provided?</td>
</tr>
<tr>
<td></td>
<td>How do you ensure that the listing of individuals who need to complete the training is up-to-date (new faculty/staff are added and individuals who leave Stanford are removed)?</td>
</tr>
<tr>
<td></td>
<td>Does the level of training vary depending on the responsibilities of the recipient?</td>
</tr>
<tr>
<td></td>
<td>Has training been updated to reflect regulatory changes, new developments and/or emerging compliance issues? If so, how?</td>
</tr>
</tbody>
</table>

### Data Collection Form – 8

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>5. Monitoring, Auditing, and Systems for Reporting Suspected Wrongdoing</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>A. Monitoring</td>
</tr>
<tr>
<td></td>
<td>How does your compliance area monitor that regulatory requirements and related P&amp;P are in effect and being adhered to?</td>
</tr>
<tr>
<td></td>
<td>Does your compliance area perform self-assessments of compliance? If so, how often? What monitoring results are collected, and to whom are they reported?</td>
</tr>
</tbody>
</table>

### Data Collection Form – 9

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>6. Accreditations/ Certifications/ Licenses</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Please provide a list of current university accreditations, certifications, and/or licenses, if any, within your compliance area.</td>
</tr>
<tr>
<td></td>
<td>Please include the accrediting/licensing body for the list of accreditations, certifications, and/or licenses listed above.</td>
</tr>
<tr>
<td></td>
<td>What is the frequency that the above accreditation/license is performed or required?</td>
</tr>
</tbody>
</table>
Data Collection Form – 10

A. AUDITING

i. Has there been any external audit activity in the last three years? If so, when? Attach copies of applicable reports and corrective plans, if any.

ii. Have external consultant(s) been used in your compliance area to review data/information, contracts, phones, etc. in the last three years? If so, please describe.

iii. Has there been any internal audit activity in the last three years? If so, when?

Data Collection Form – 11

B. SYSTEMS FOR REPORTING SUSPECTED WRONGDOING

i. Are your faculty and staff aware that Stanford has a reporting mechanism for suspected wrongdoing (e.g., the compliance hotline, Office of the General Counsel, Office of the Ombuds and/or Human Resources Department, etc.)? If so, how are personnel in your compliance area informed of such avenues for reporting concerns?

ii. Does your compliance area have any additional mechanisms for reporting concerns (e.g., hotlines, email, etc.)?

Data Collection Form – 12

C. CONSISTENT ENFORCEMENT AND APPROPRIATE DISCIPLINE

i. Do P&P outline consequences for noncompliance with regulatory requirements and policies?

ii. If a FCPA notice consequence for noncompliance with regulatory requirements and policies?

D. RESPONDING TO NONCOMPLIANCE AND MODIFYING THE PROGRAM AS NECESSARY

i. Has it been necessary to modify processes or controls, or retrain individuals responsible, etc. to address non-compliance in the past year? If so, please explain.
Additional Comments/Concerns in Your Compliance Area?

- Is your compliance area planning any strategic objectives or upcoming changes (e.g., physical location changes, software changes, organizational restructuring, etc.)? Please describe below.

Compliance Risk Assessments (CRAs)

Compliance Risk Assessments - Purpose

**Compliance Risk Assessment Methodology**

- (Revised February 2015)

  - Risk assessments are a key element of an effective compliance and ethics program. Stanford’s Compliance and Ethics Program is made up of 26 distinct risk areas. The Compliance and Ethics Program is engaged in an effort to conduct assessments of these compliance areas to ensure compliance risk is being properly managed across the University.

- Cost.
Compliance Risk Assessment (CRA) - Template

Compliance Risk Assessment

Executive Summary

- Introduction
- Background
  - Regulations regarding _______ and related matters are listed in Attachment A.

Scope

- The Office of Compliance and Ethics (OCE) researched recent case studies and governmental enforcement of __________.
- A list of federal enforcement actions is included in Attachment B.
- This assessment has identified _#_ sub-risks related to __________ in the table below.

<table>
<thead>
<tr>
<th>Sub Risk</th>
<th>Reviewed on Attachment</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Attachment C</td>
</tr>
<tr>
<td>2</td>
<td>Attachment D</td>
</tr>
</tbody>
</table>

Work Performed

- The Office of Compliance and Ethics interviewed individuals and offices who have responsibilities in managing and ownership of _______. Those Offices include:
  - _______ and _______.

Conclusion
Observations and Recommendations

The following observations were discussed with the owner of __________. Please see Attachment E for a list of observations, recommendations and management action plans.

• Observation 1
• Observation 2

For each of the observations above, the following recommendations were made:

• Recommendation 1
• Recommendation 2

(Signature on file)

• Mary Jane, Chief Ethics and Compliance Officer

Performed By:

• Joe Doe, Compliance Program Manager

List of Attachments

1. Attachment A – Rules and Regulations
2. Attachment B – Enforcement Actions and Case Studies
3. Attachment C – Sub Risk 1
4. Attachment D – Sub Risk 2
5. Attachment E – Management Action Plan (MAP)
Federal Enforcement Actions

<table>
<thead>
<tr>
<th>University Sub-Risk Area</th>
<th>University / College</th>
<th>Year</th>
<th>Issue</th>
</tr>
</thead>
</table>

CRA – Template - Attachment C – Sub-risk 1

Sub-risk 1: _____________________________

Owners:

- Standards and procedures:
  - Stanford policies and procedures addressing ____________ are found in:
    - Stanford University Administrative Guide
      - Policy 1
      - Policy 2

- Governance, organization and reporting:
  - Efforts to include only personnel who have engaged in appropriate conduct.
  - Use partial list of the internal and a "best practices" list to include management of the role to identify people in the role and any specific actions that are necessary for their role.
  - This includes personnel in positions of substantial authority and trust, too.

- Training and education:
  - Stanford ensures that functional risk owners and their staff continue to be appropriately trained to fulfill their responsibilities, including staying current with regulatory requirements in their area. Activities include:
    - Program monitoring and auditing, evaluating program effectiveness, and systems for reporting suspected wrongdoing.
    - Systems for reporting suspected wrongdoing:
      - Concerns with ____________ can be reported by:
        - As with any concerns, the University’s Office of Health Compliance, Risk and Privacy is available for reporting concerns through its hotline or website, in person or online.
        - Employees can also speak to their supervisor, manager, or other management personnel within their department. A member of the community can also reach the Office of the General Counsel, Office of the President or University Human Resources. Stanford does not tolerate retaliation for raising such concerns in good faith.
Consistent enforcement and appropriate discipline.

Stanford University takes laws and regulations very seriously, and the safety and security of students, faculty and other members of the Stanford community. Every effort is made to ensure appropriate discipline and enforcement when necessary.

Responding to noncompliance and modifying the program as necessary.

Sub-Risk 2: Owners:

1. Standards and procedures.
   - University policies and procedures addressing __________ are found in Stanford University Administrative Guide, adminguide.stanford.edu, Policy 1, Policy 2.

2. Governance, organization and reporting.

CRA – Template - Attachment E (MAP)

<table>
<thead>
<tr>
<th>Observation</th>
<th>Recommendations</th>
<th>Completion Date</th>
<th>Responsible Party</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
CRA – Follow-up

Perform a Follow-up of Recommendations made
❖ As and when Management Action Plan (MAP) is due.

Report to:
❖ Audit, Compliance and Risk Committee, and/or
❖ Senior Management.

Questions

Contact Information
Sonal J. Shah, CPA, MSPA, CHC, CGMA
Chief Ethics and Compliance Officer
Stanford University
616 Serra Street | Room 10 | Encina Hall | Stanford, CA 94305 | (650) 723-3267 | sshah3@stanford.edu
acrp.stanford.edu | Compliance and Ethics Helpline | helpline.stanford.edu