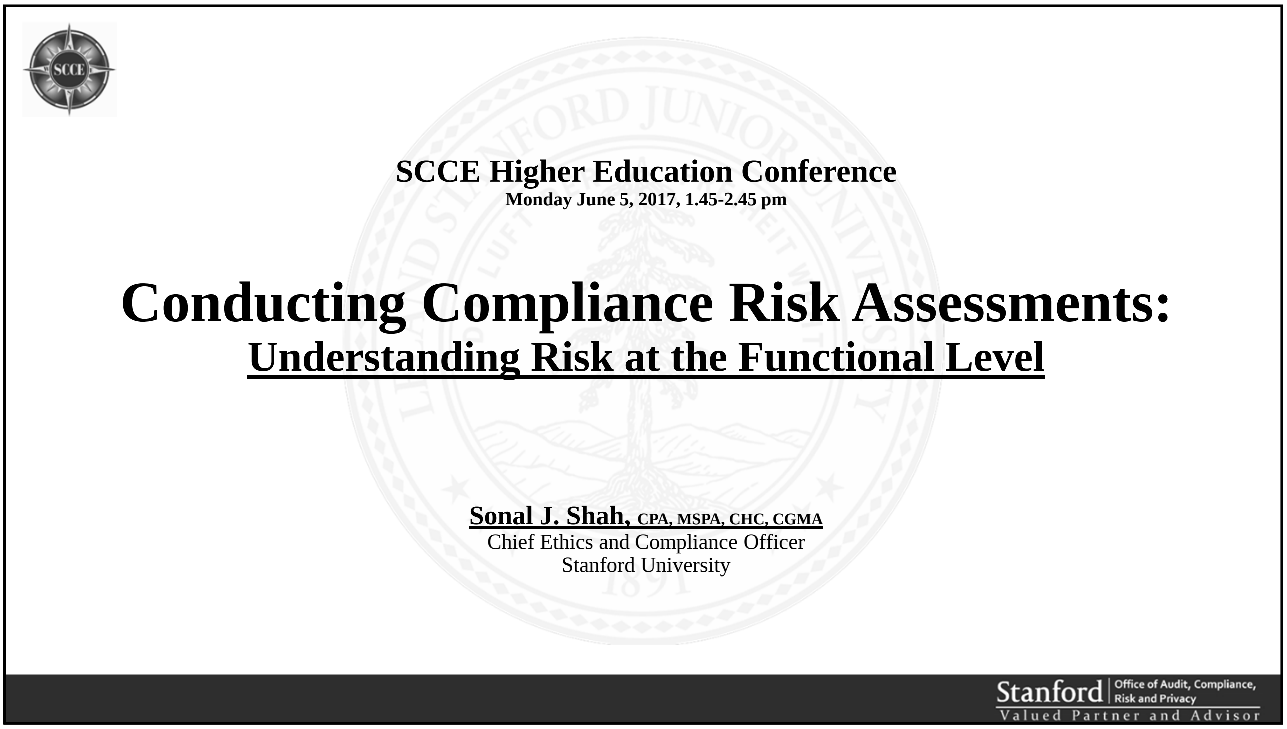


SCCE Higher Education Conference

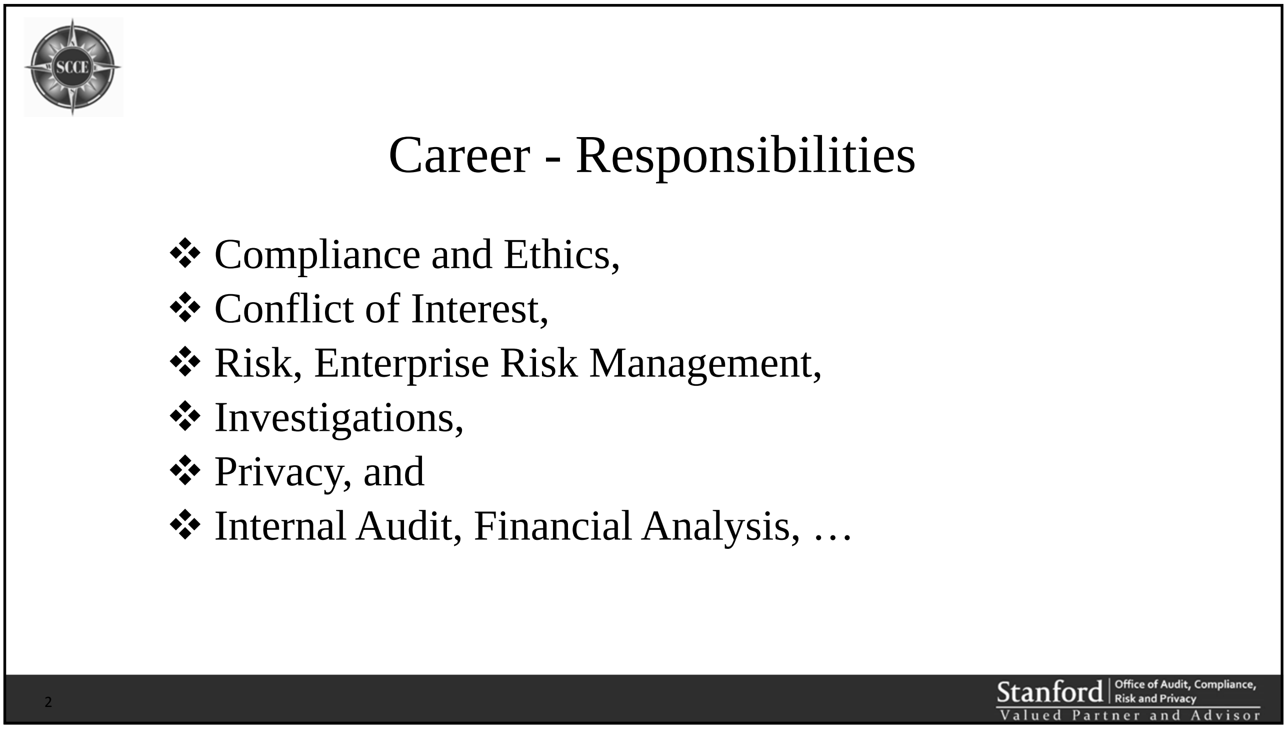
Monday June 5, 2017, 1.45-2.45 pm

Conducting Compliance Risk Assessments:

Understanding Risk at the Functional Level

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

Stanford | Office of Audit, Compliance, Risk and Privacy
Valued Partner and Advisor

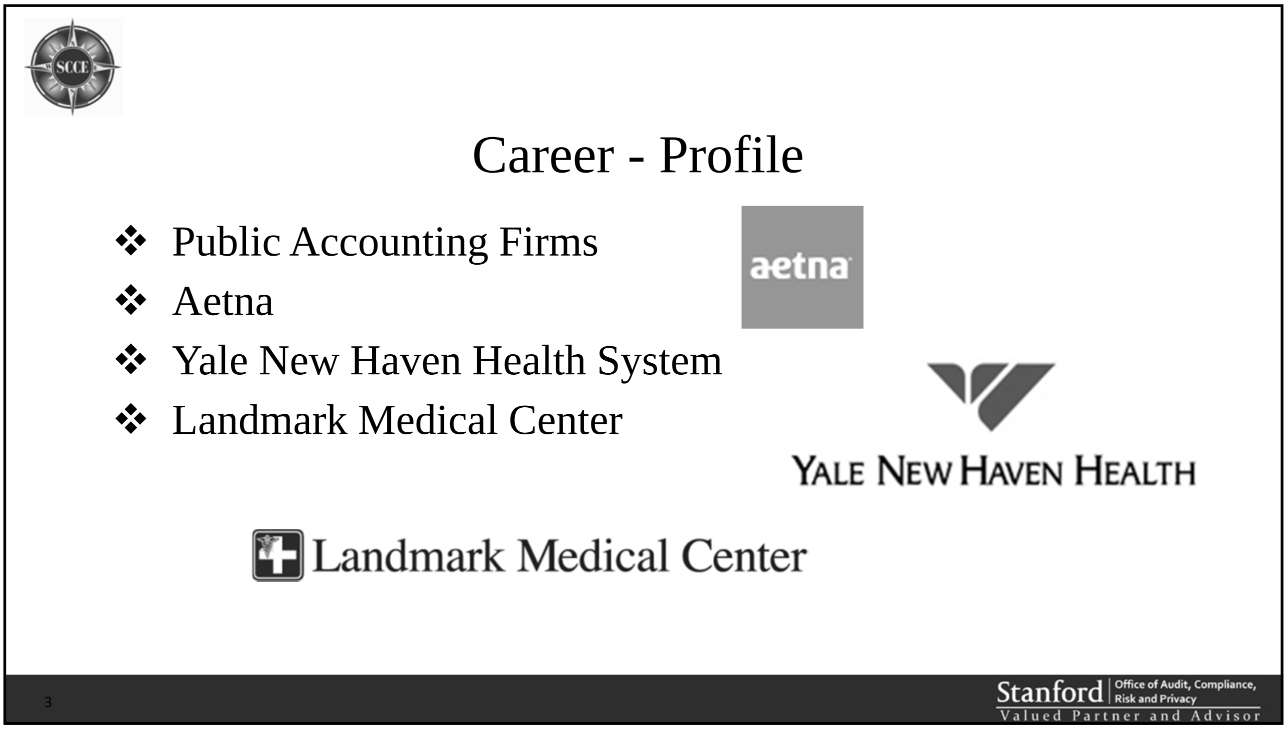


Career - Responsibilities

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

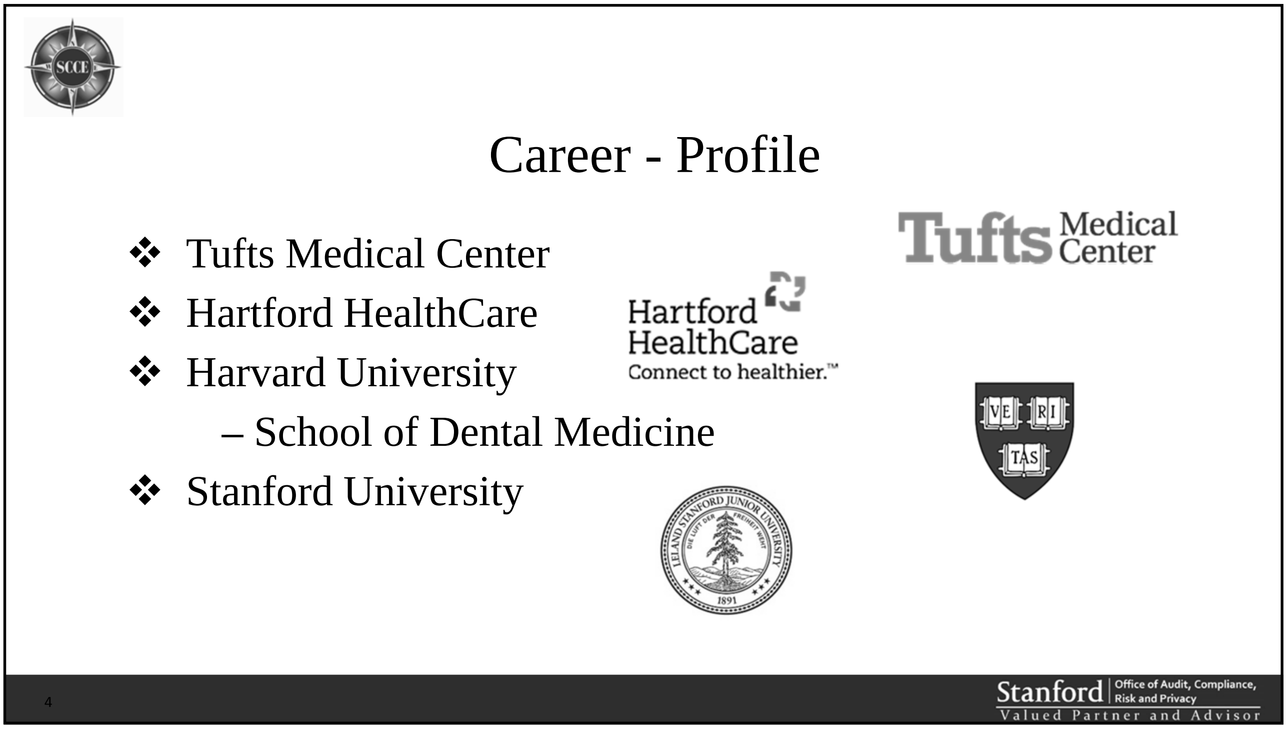
2

Stanford | Office of Audit, Compliance, Risk and Privacy
Valued Partner and Advisor


SCCE
aetna
YALE NEW HAVEN HEALTH
Landmark Medical Center

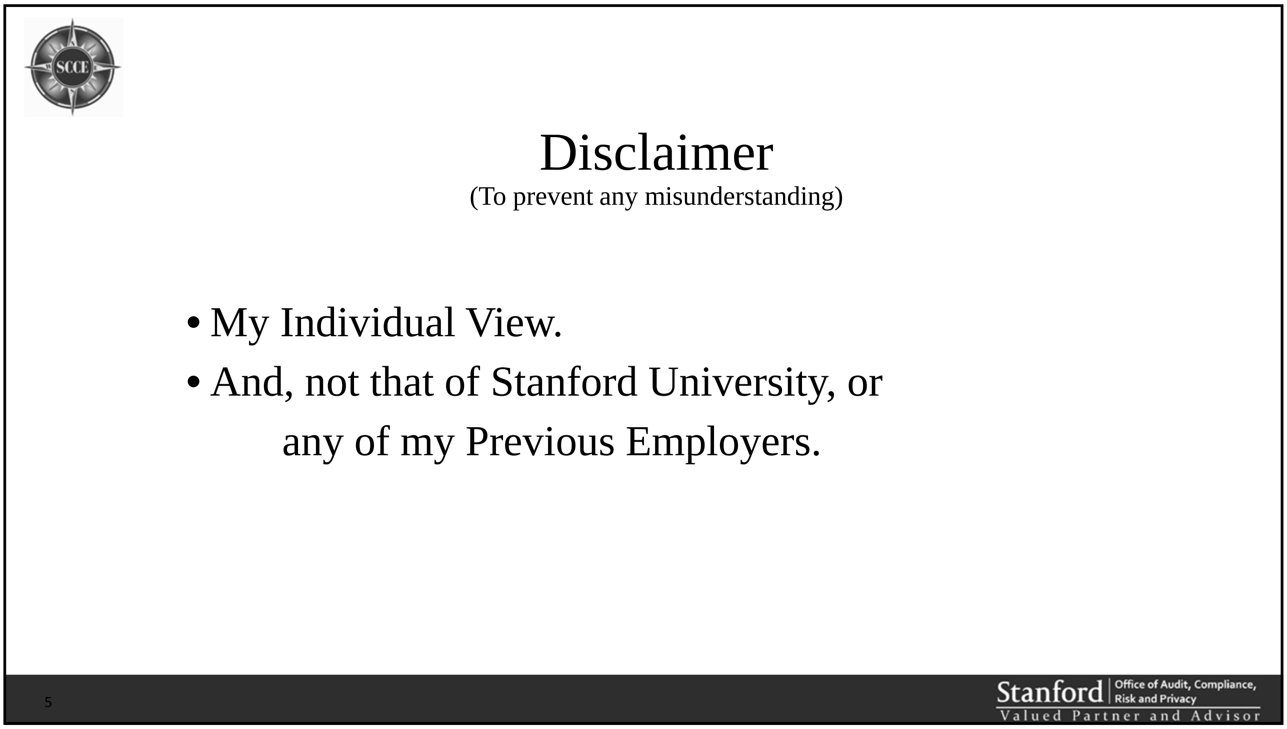
Career - Profile

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


SCCE
Tufts Medical Center
Hartford HealthCare
Connect to healthier.™
VE RI TAS
LELAND STANFORD JUNIOR UNIVERSITY
DIE LUFT DER FREIHEIT WEHT
1891

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

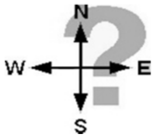
By a Show of Hands…

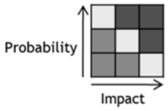
How many would say that they have

- an “Evolving” Compliance Program

vs.

- a “Mature” Compliance Program?





How about

- A Structured/formal Enterprise Risk Management Program?

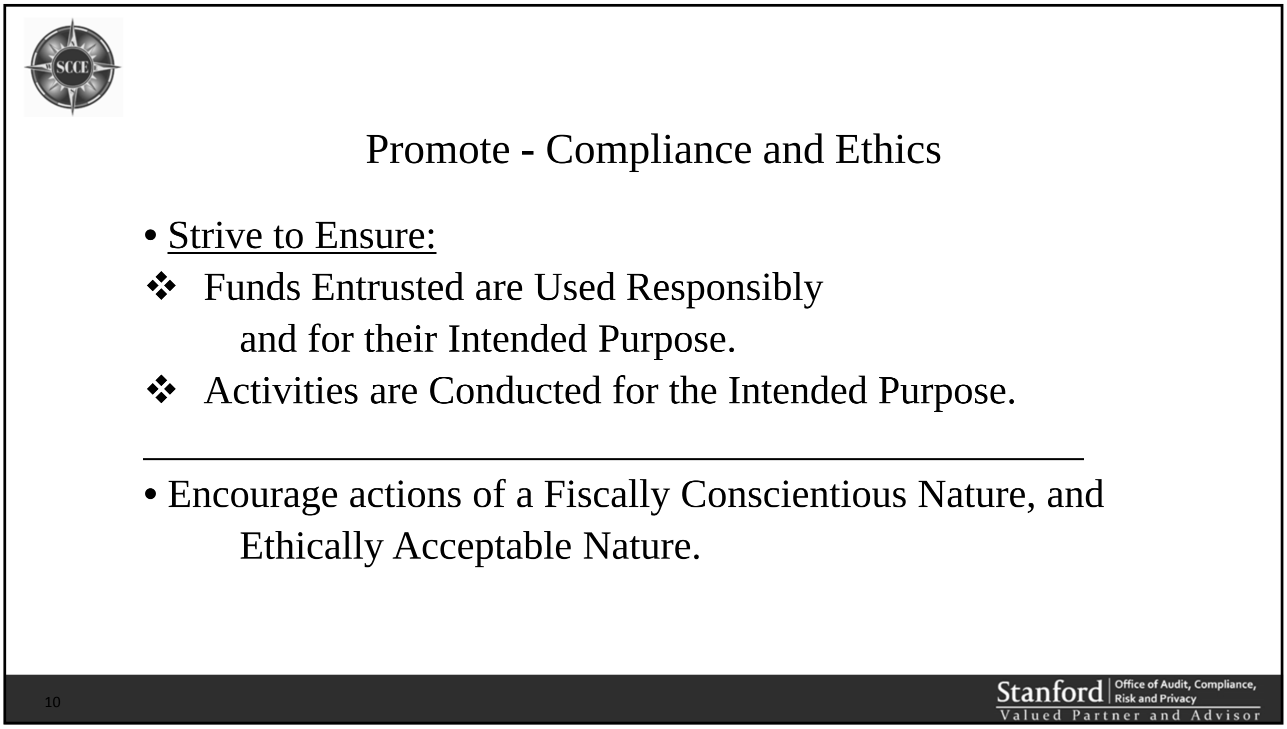
Stanford University’s Program

Stanford | Office of Audit, Compliance, Risk and Privacy

Valued Partner and Advisor

University - Not-for-Profit World – Stakeholders

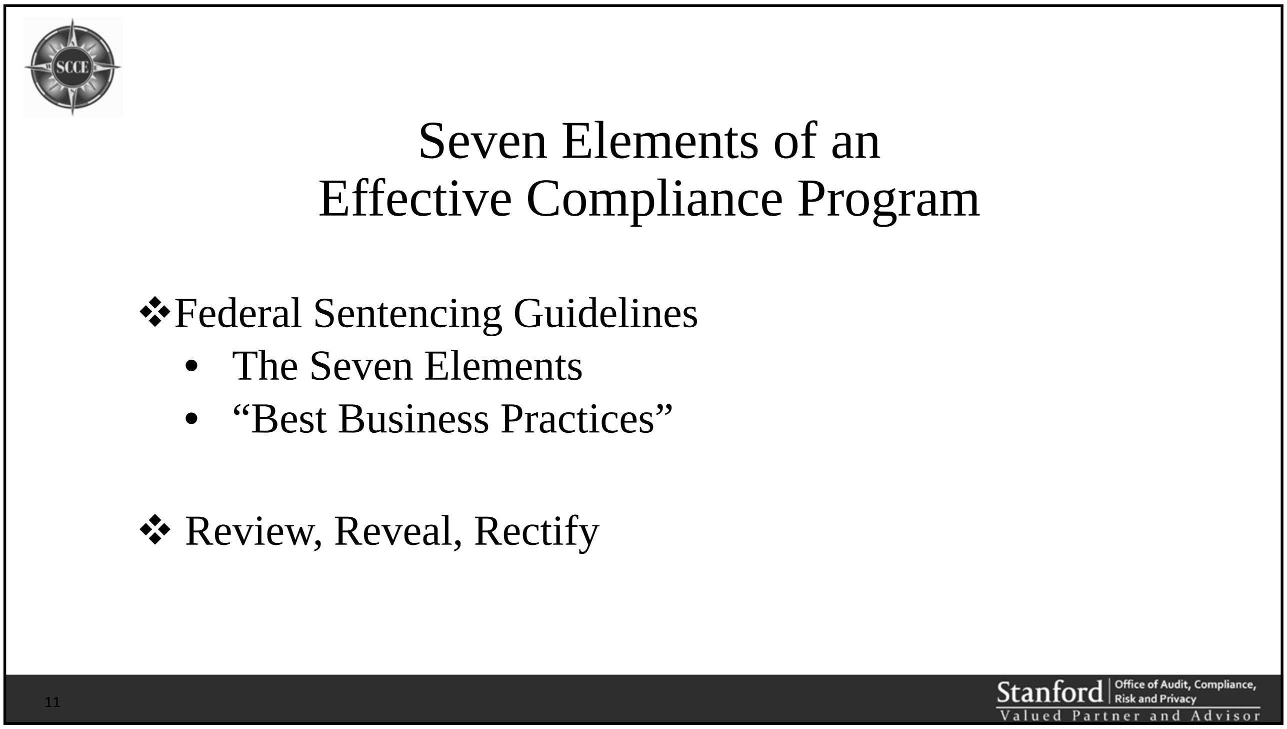
- ❖ Students
  - Education and Learning
- ❖ Governmental and Private Sponsors
  - Research
- ❖ Donors
  - Various Causes and Activities
- ❖ Patients and Insurers
  - Patient Care



Promote - Compliance and Ethics

- <u>Strive to Ensure:</u>
- ❖ Funds Entrusted are Used Responsibly and for their Intended Purpose.
- ❖ Activities are Conducted for the Intended Purpose.

- Encourage actions of a Fiscally Conscientious Nature, and Ethically Acceptable Nature.



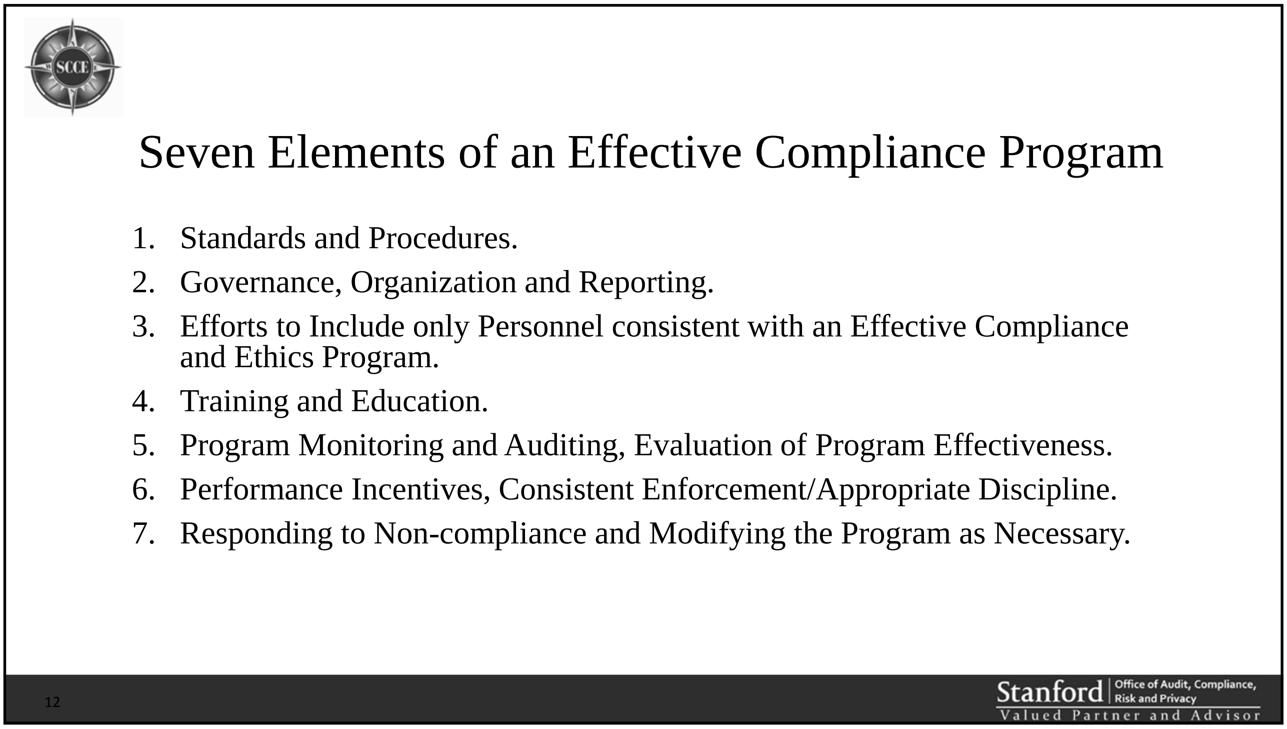
Seven Elements of an Effective Compliance Program

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

❖ Review, Reveal, Rectify

11

Stanford | Office of Audit, Compliance, Risk and Privacy
Valued Partner and Advisor

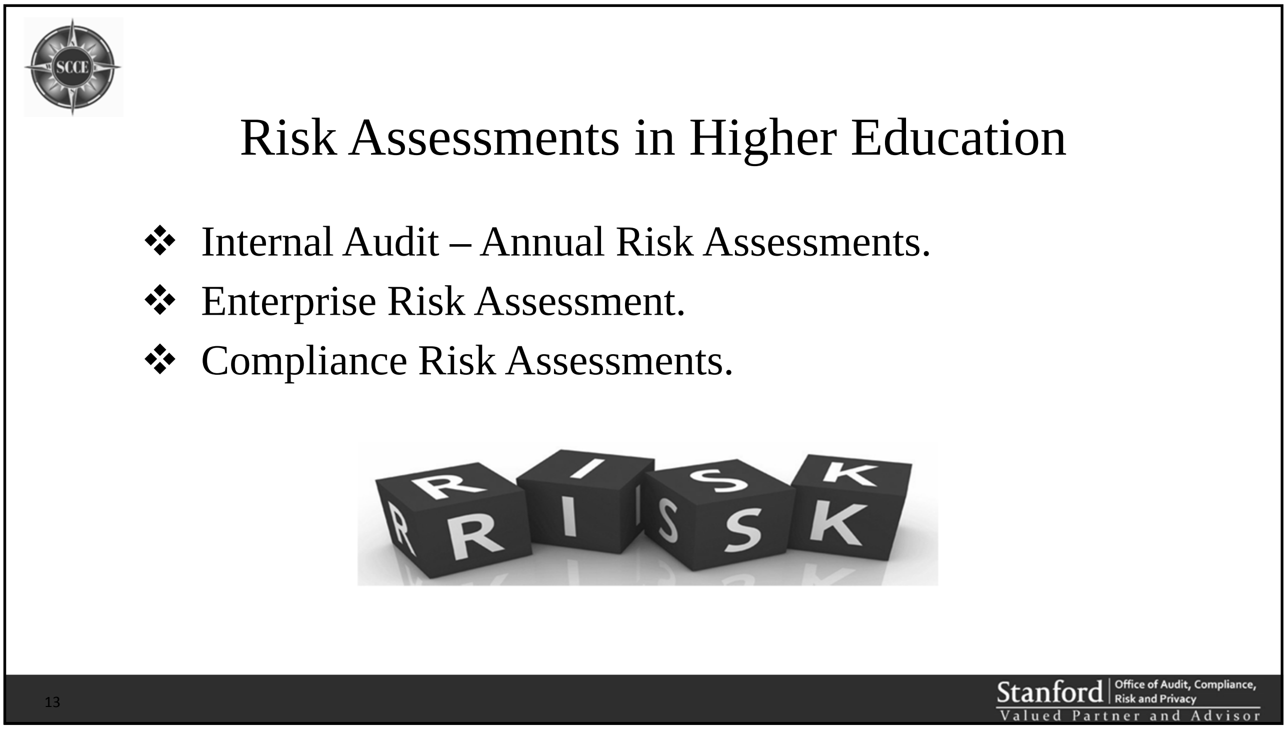


Seven Elements of an Effective Compliance Program

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.

12

Stanford | Office of Audit, Compliance, Risk and Privacy
Valued Partner and Advisor

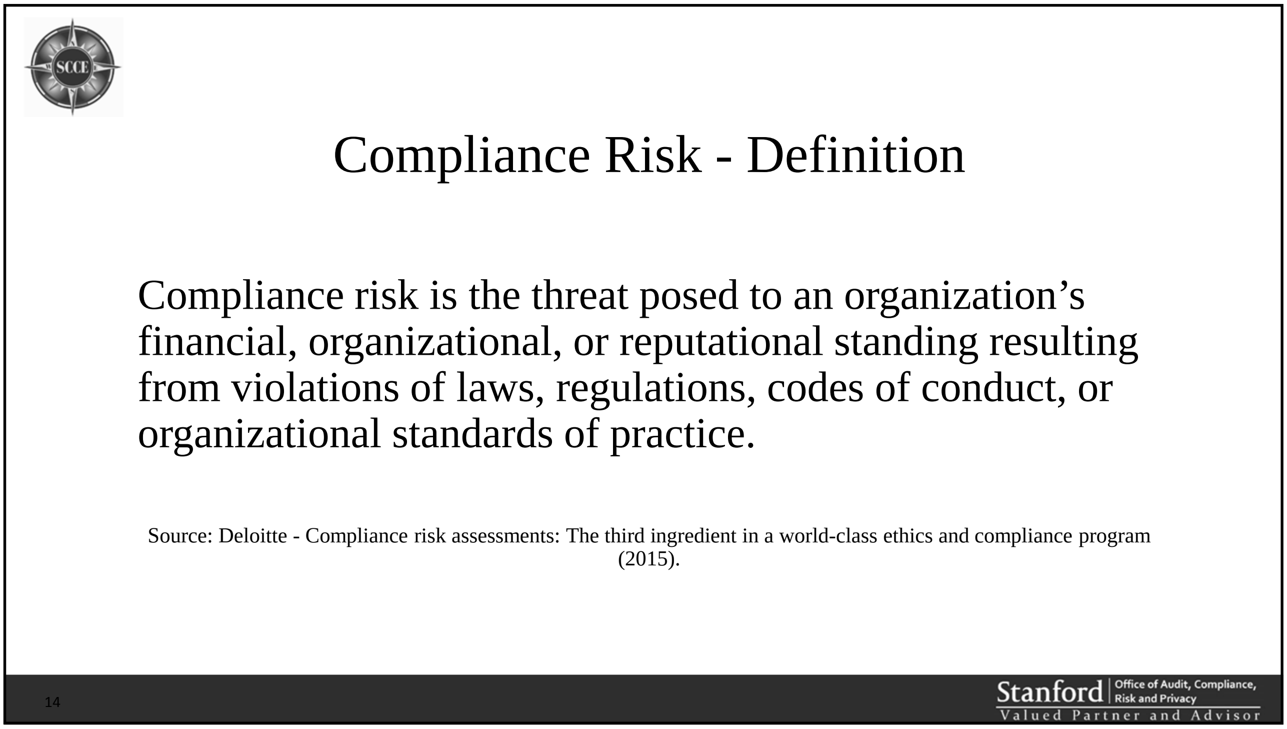


Risk Assessments in Higher Education

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

13

Stanford | Office of Audit, Compliance, Risk and Privacy
Valued Partner and Advisor



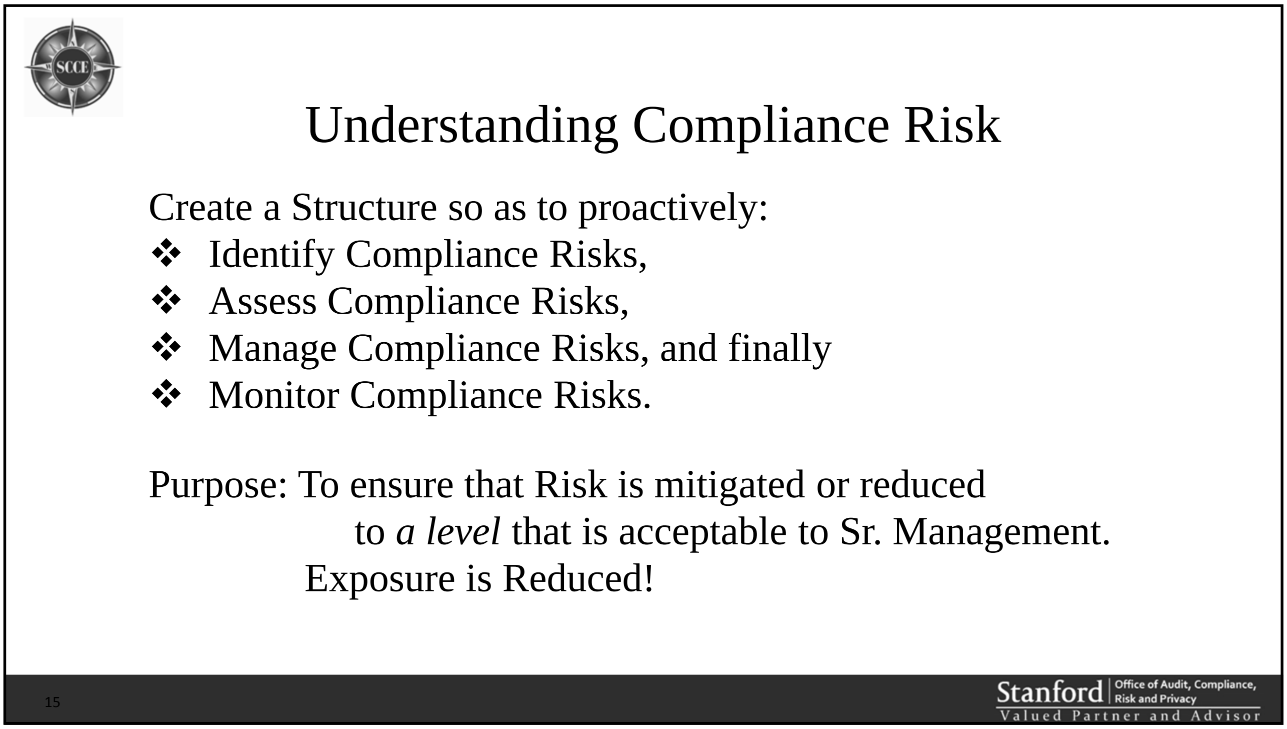
Compliance Risk - Definition

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).

14

Stanford | Office of Audit, Compliance, Risk and Privacy
Valued Partner and Advisor



Understanding Compliance Risk

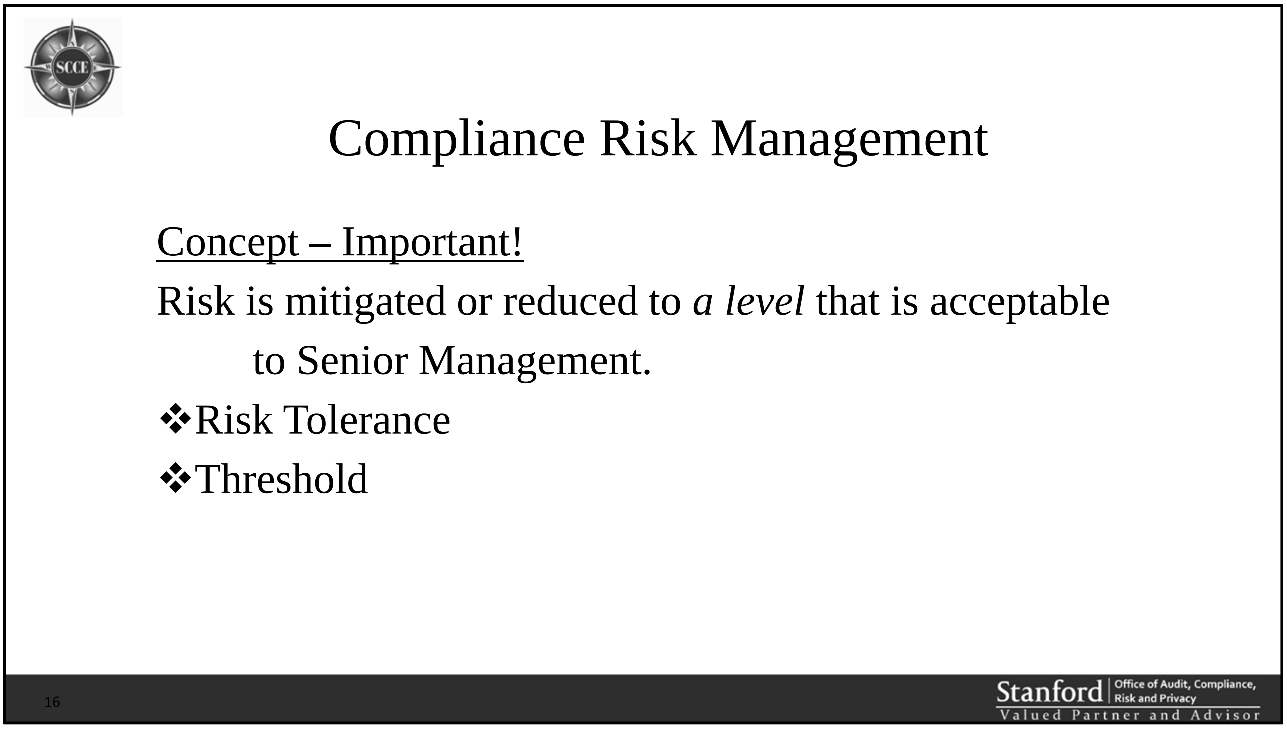
Create a Structure so as to proactively:

- ❖ 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!

15

Stanford | Office of Audit, Compliance, Risk and Privacy
Valued Partner and Advisor



Compliance Risk Management

Concept – Important!

Risk is mitigated or reduced to *a level* that is acceptable to Senior Management.

- ❖Risk Tolerance
- ❖Threshold

16

Stanford | Office of Audit, Compliance, Risk and Privacy
Valued Partner and Advisor

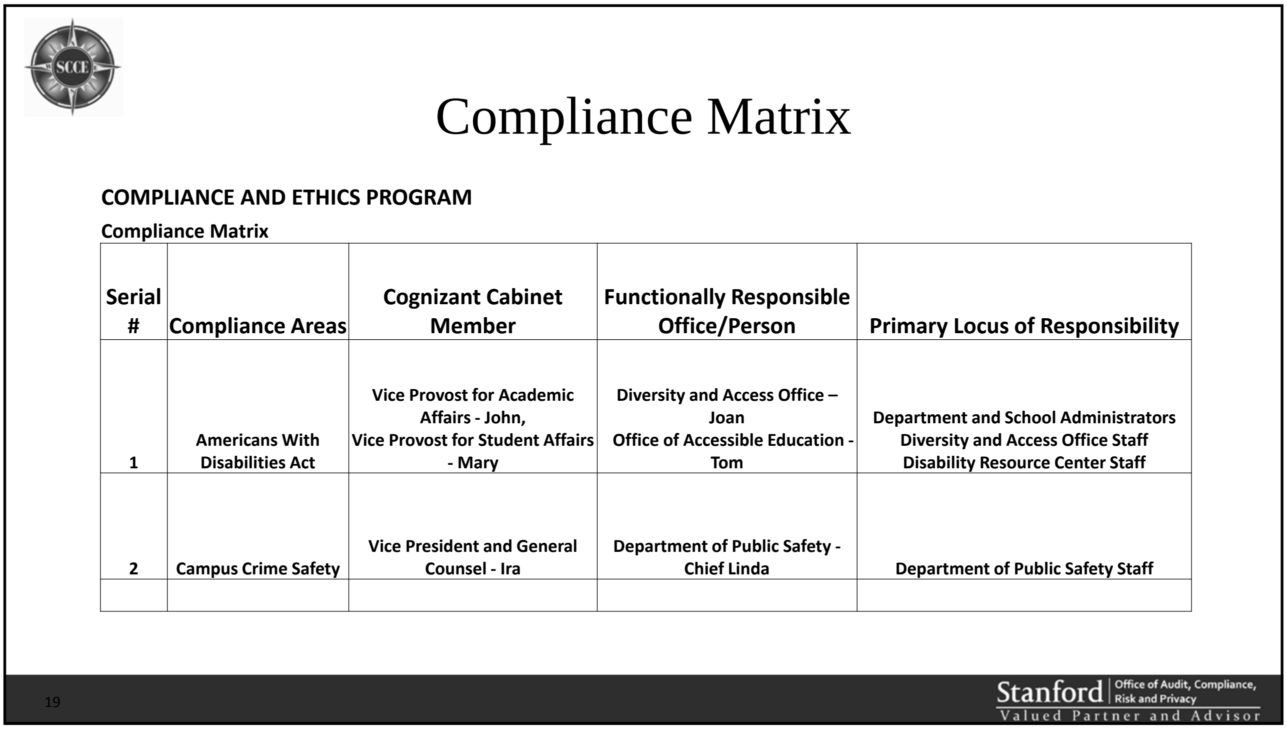
Compliance Risk Management

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.

- ❖ Emphasize – Responsibility for Compliance - stays with Sr. Management Risk Owner and Functional Risk Owner.

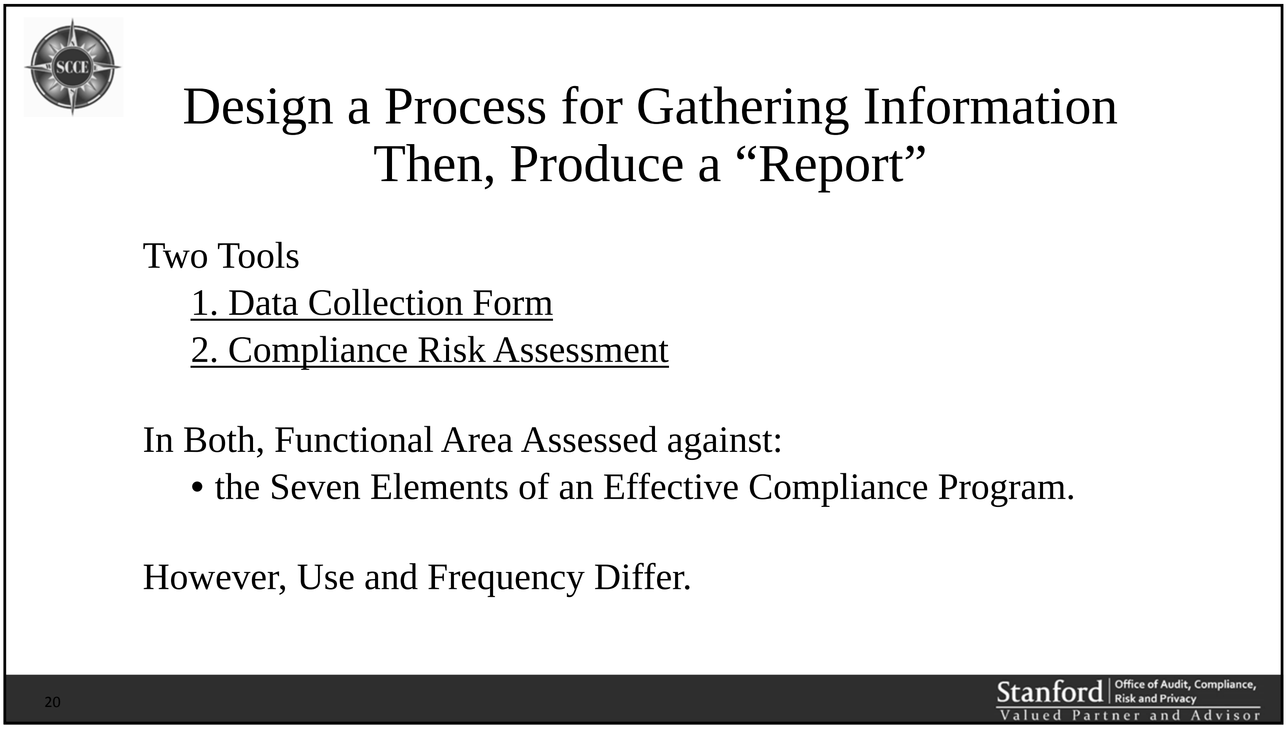


Compliance Matrix

COMPLIANCE AND ETHICS PROGRAM

Compliance Matrix

Serial #	Compliance Areas	Cognizant Cabinet Member	Functionally Responsible Office/Person	Primary Locus of Responsibility
1	Americans With Disabilities Act	Vice Provost for Academic Affairs - John, Vice Provost for Student Affairs - Mary	Diversity and Access Office – Joan Office of Accessible Education - Tom	Department and School Administrators Diversity and Access Office Staff Disability Resource Center Staff
2	Campus Crime Safety	Vice President and General Counsel - Ira	Department of Public Safety - Chief Linda	Department of Public Safety Staff



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 Forms

Data Collection Form - 1

A.	**RULES, REGULATIONS, AND OTHER REGULATORY REQUIREMENTS**
i.	**Please list all relevant <u>federal</u> laws/ regulations that apply to your compliance area, if any.**
i.	**Please list all relevant <u>state</u> laws/ regulations that apply to your compliance area, if any.**
i.	**Please list all relevant <u>local</u> laws/ regulations that apply to your compliance area, if any.**
i.	**Please list all other sources for guidance/ best practices (e.g. professional organizations, journal subscriptions, listservs, etc.), if any.**

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.

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

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

Data Collection Form – 3

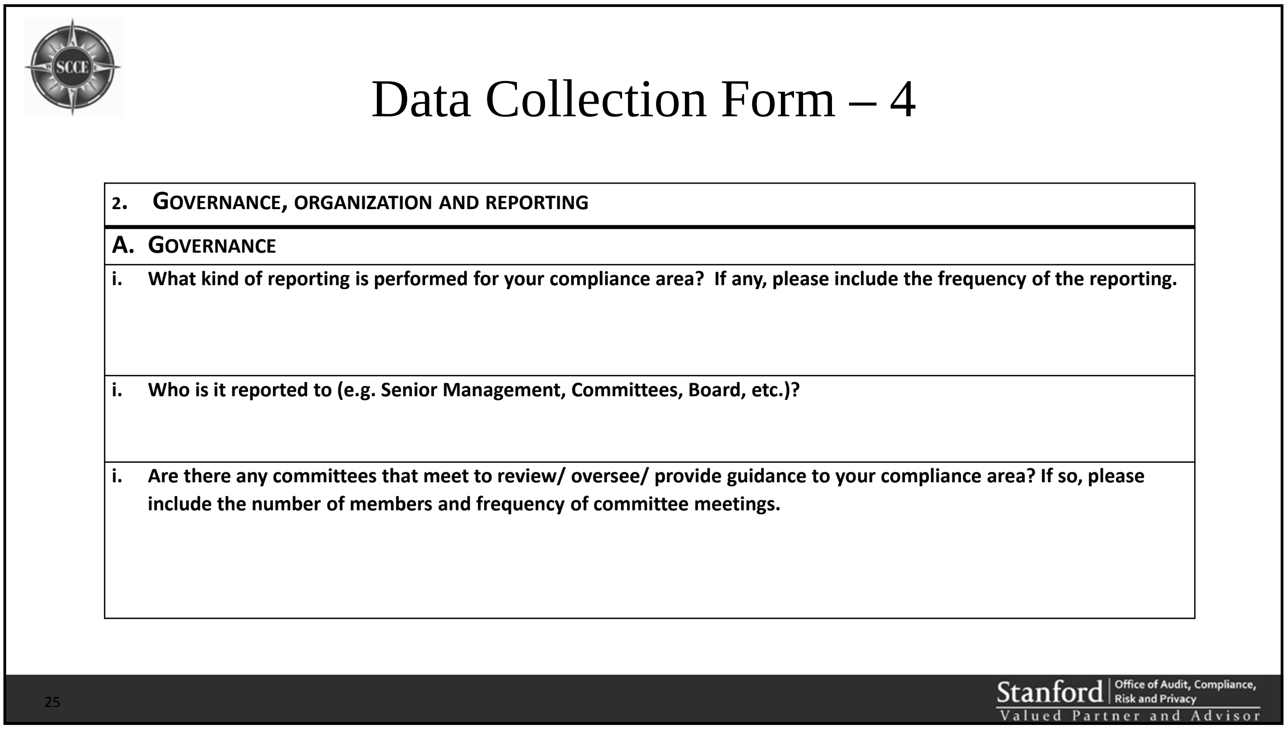
Seven Elements of an
Effective Compliance and Ethics Program

The seven elements are set out in the Federal Sentencing Guidelines (FSG) for organizations. Although these criteria have their origin 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 Ethics and emphasized promoting an ethical business culture, beyond simply compliance with laws.

1. Standards and Procedures

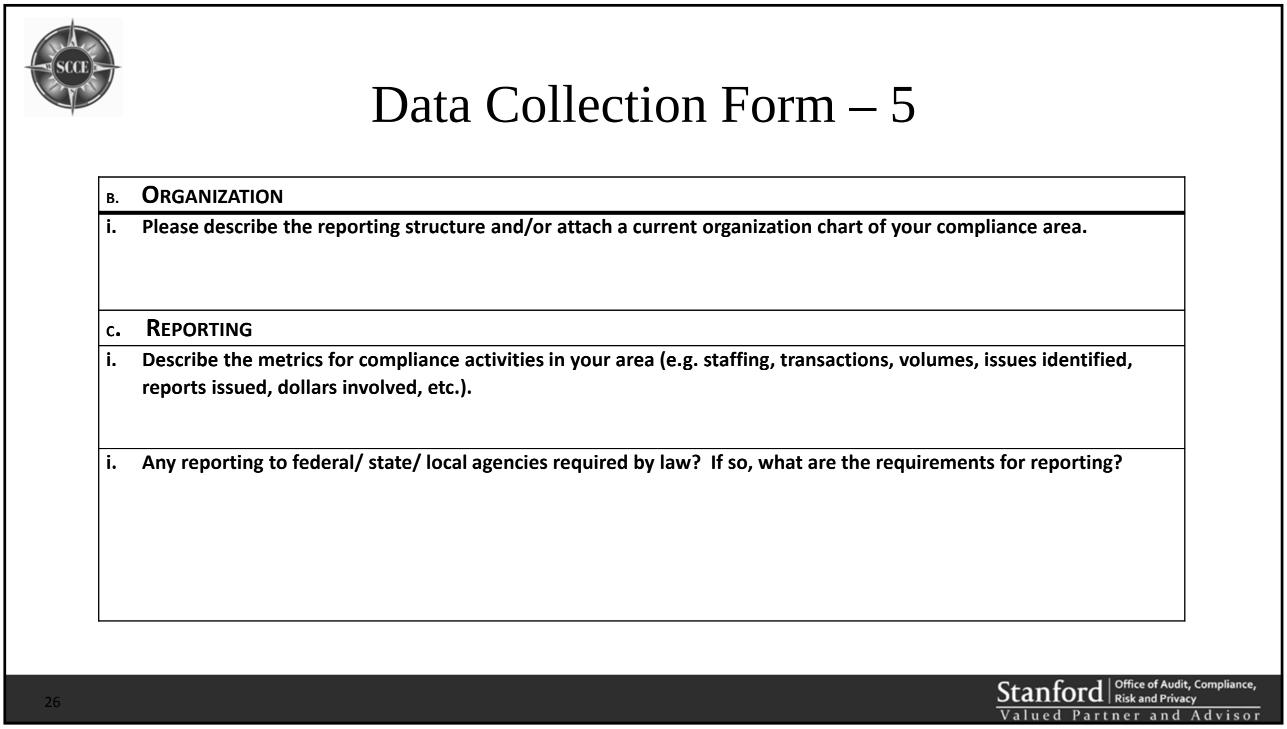
i. Please provide hyperlinks or attachments to all relevant Policies and Procedures (P&P) in your compliance area. If several P&P exist, is there one hyperlink that provides access to all relevant P&P?

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



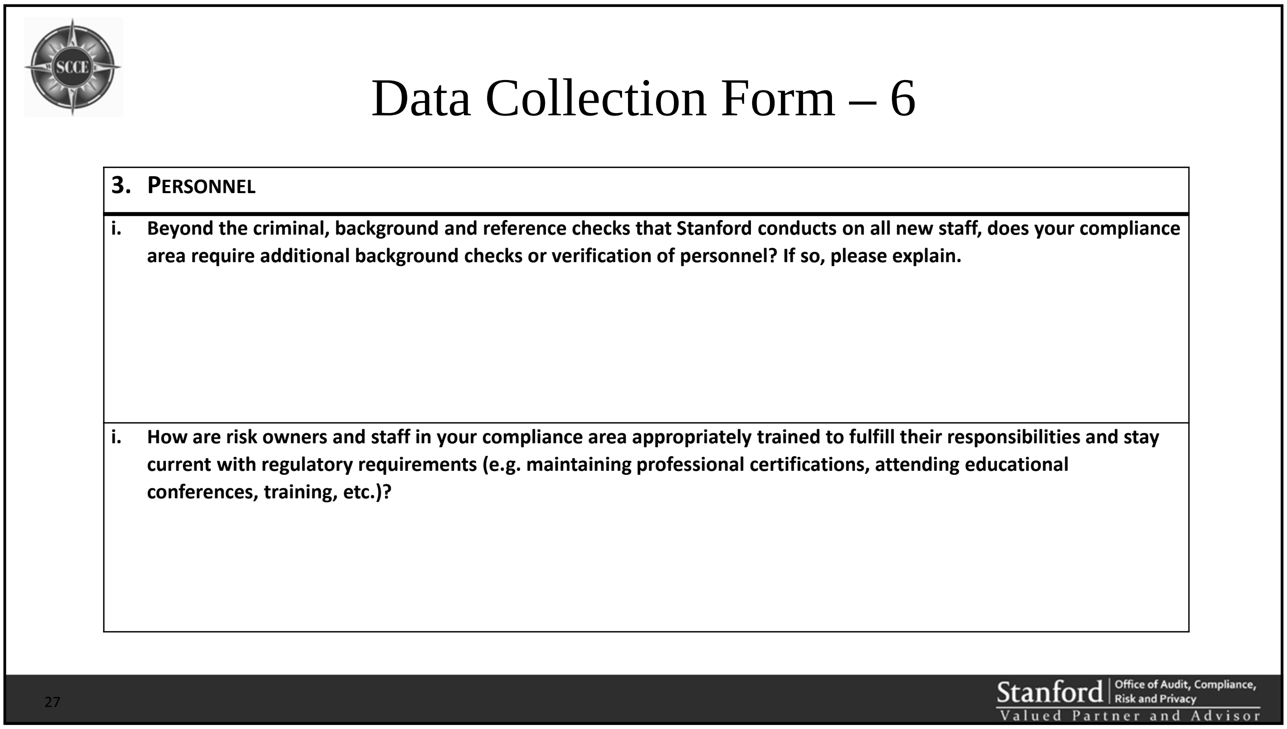
Data Collection Form – 4

2.	**GOVERNANCE, ORGANIZATION AND REPORTING**
A.	**GOVERNANCE**
i.	**What kind of reporting is performed for your compliance area? If any, please include the frequency of the reporting.**
i.	**Who is it reported to (e.g. Senior Management, Committees, Board, etc.)?**
i.	**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.**



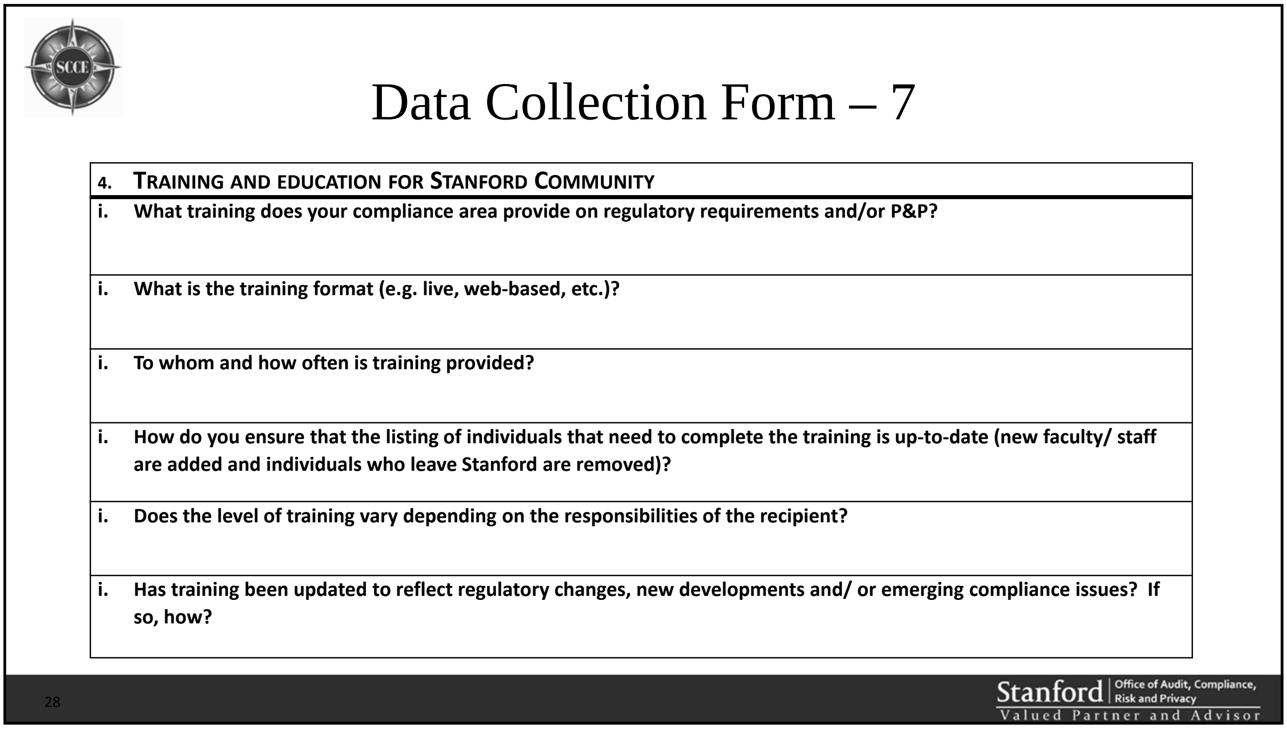
Data Collection Form – 5

B.	**ORGANIZATION**
i.	**Please describe the reporting structure and/or attach a current organization chart of your compliance area.**
C.	**REPORTING**
i.	**Describe the metrics for compliance activities in your area (e.g. staffing, transactions, volumes, issues identified, reports issued, dollars involved, etc.).**
i.	**Any reporting to federal/ state/ local agencies required by law? If so, what are the requirements for reporting?**



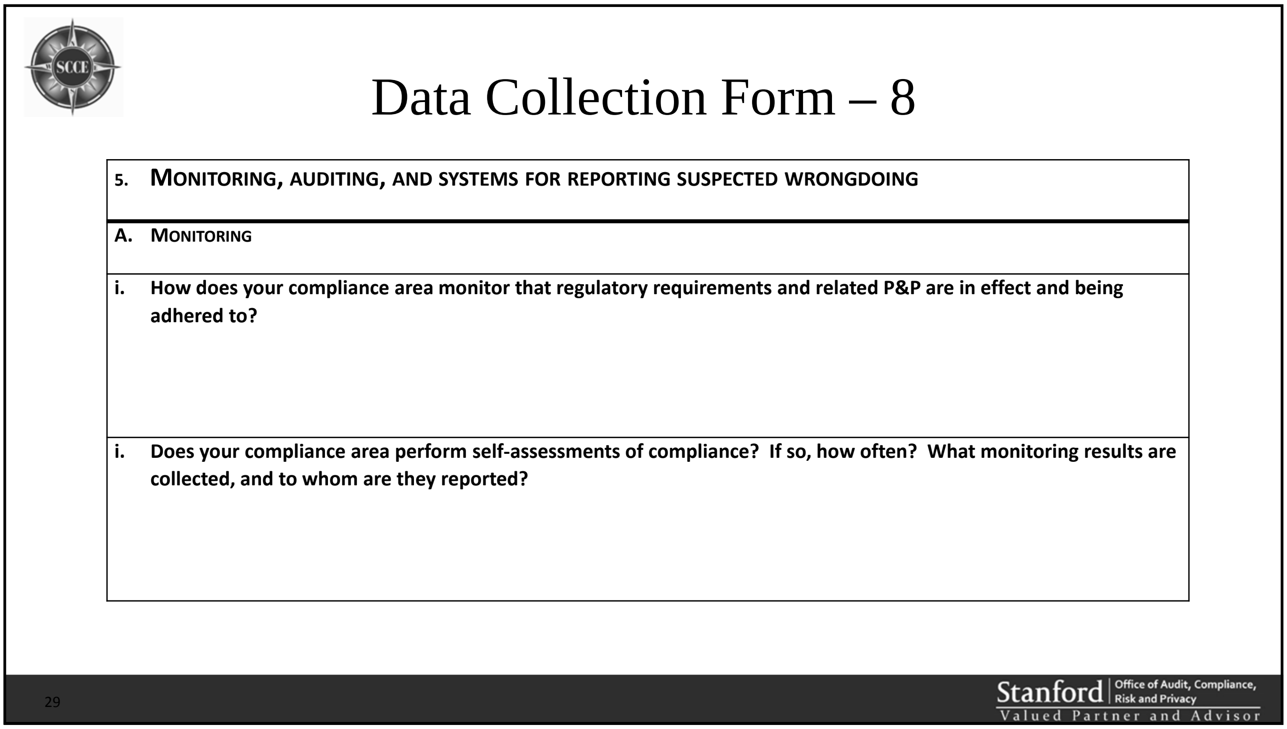
Data Collection Form – 6

3. Personnel
i. 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.
i. 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

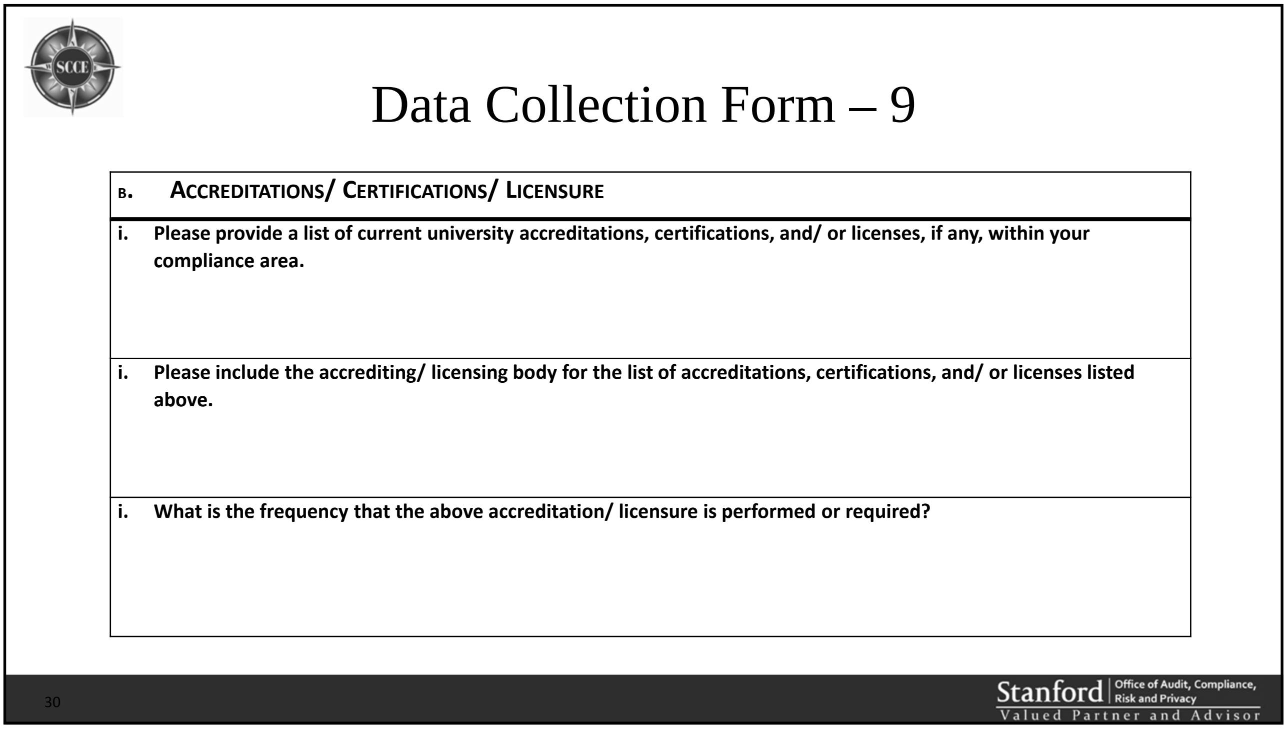
4. Training and education for Stanford Community
i. What training does your compliance area provide on regulatory requirements and/or P&P?
i. What is the training format (e.g. live, web-based, etc.)?
i. To whom and how often is training provided?
i. How do you ensure that the listing of individuals that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



Data Collection Form – 8

5.	MONITORING, AUDITING, AND SYSTEMS FOR REPORTING SUSPECTED WRONGDOING
A.	MONITORING
i.	How does your compliance area monitor that regulatory requirements and related P&P are in effect and being adhered to?
i.	Does your compliance area perform self-assessments of compliance? If so, how often? What monitoring results are collected, and to whom are they reported?

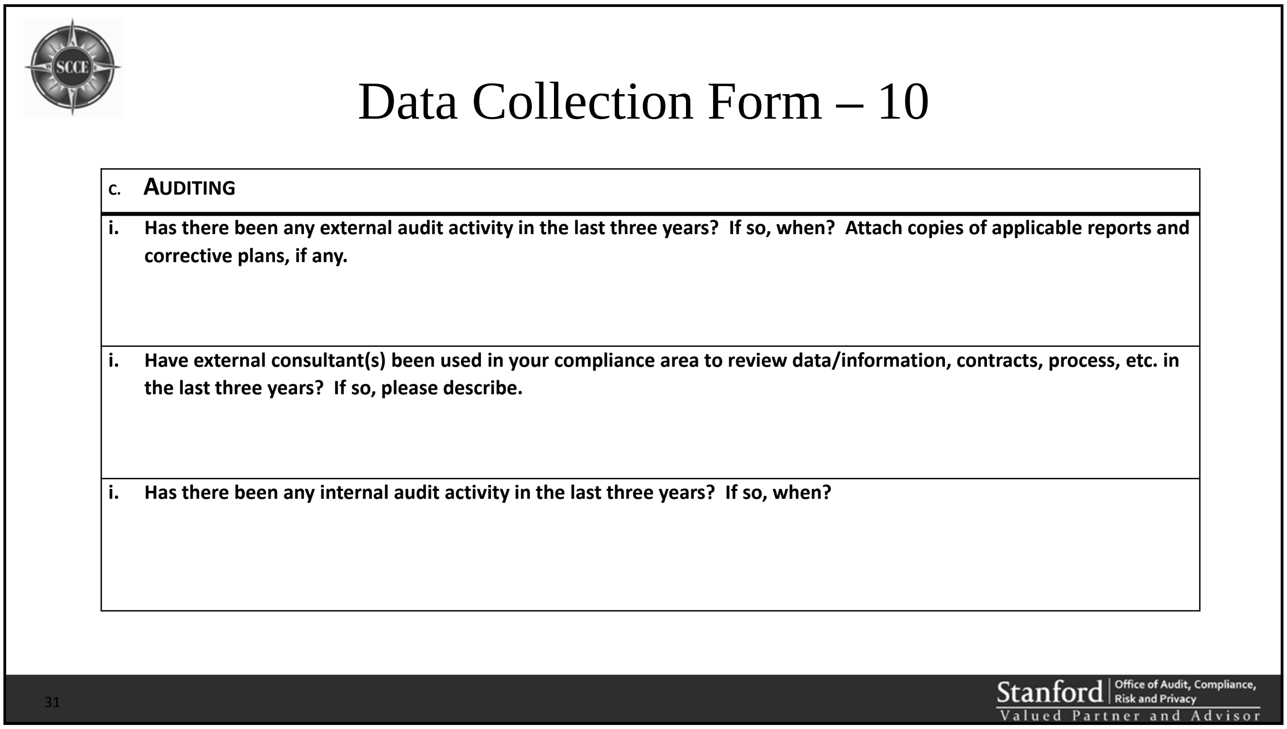
Stanford | Office of Audit, Compliance, Risk and Privacy
Valued Partner and Advisor



Data Collection Form – 9

B.	ACCREDITATIONS/ CERTIFICATIONS/ LICENSURE
i.	Please provide a list of current university accreditations, certifications, and/ or licenses, if any, within your compliance area.
i.	Please include the accrediting/ licensing body for the list of accreditations, certifications, and/ or licenses listed above.
i.	What is the frequency that the above accreditation/ licensure is performed or required?

Stanford | Office of Audit, Compliance, Risk and Privacy
Valued Partner and Advisor

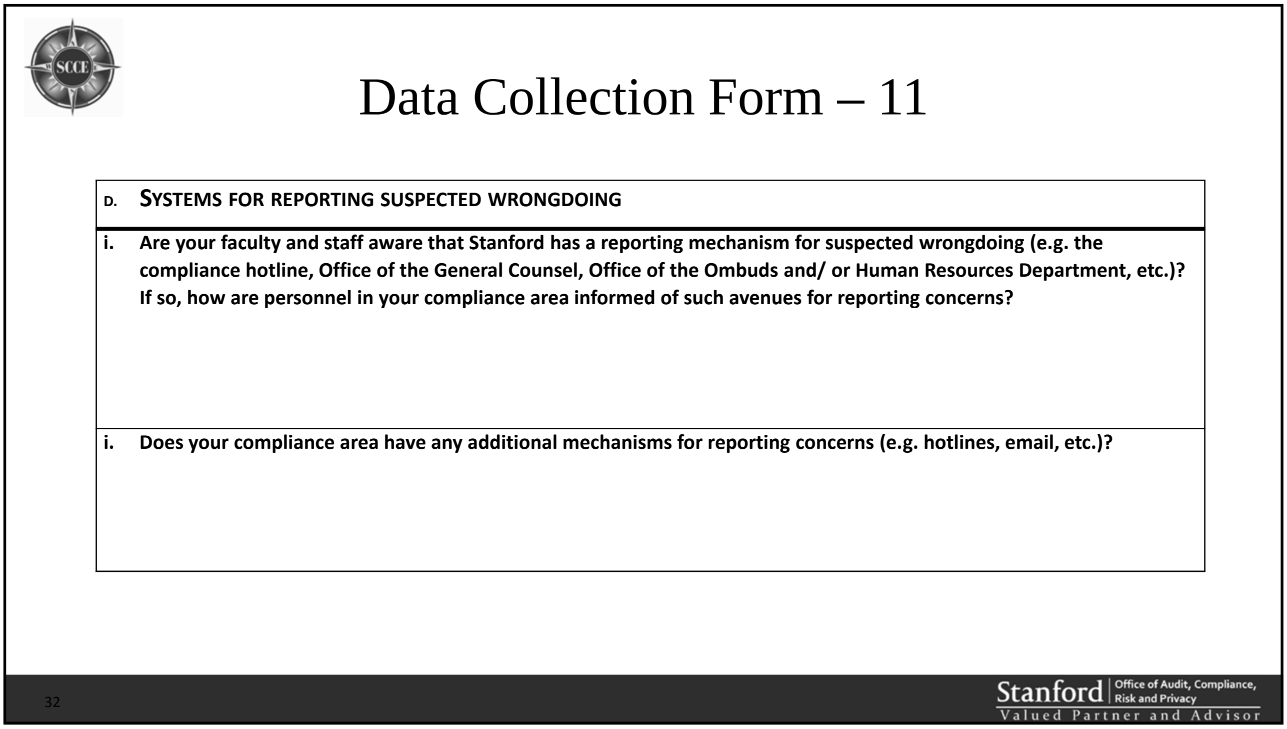


Data Collection Form – 10

C.	**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.**
i.	**Have external consultant(s) been used in your compliance area to review data/information, contracts, process, etc. in the last three years? If so, please describe.**
i.	**Has there been any internal audit activity in the last three years? If so, when?**

31

Stanford | Office of Audit, Compliance, Risk and Privacy
Valued Partner and Advisor

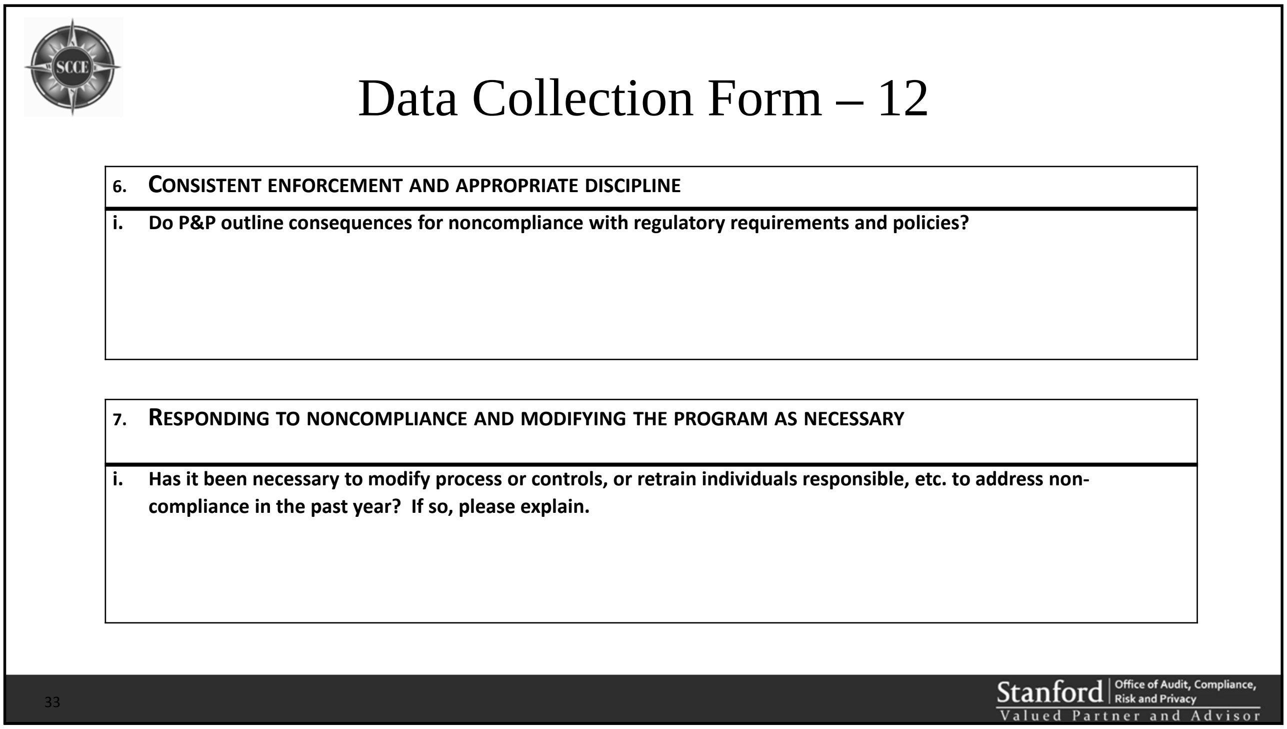


Data Collection Form – 11

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

32

Stanford | Office of Audit, Compliance, Risk and Privacy
Valued Partner and Advisor



Data Collection Form – 12

6. **CONSISTENT ENFORCEMENT AND APPROPRIATE DISCIPLINE**

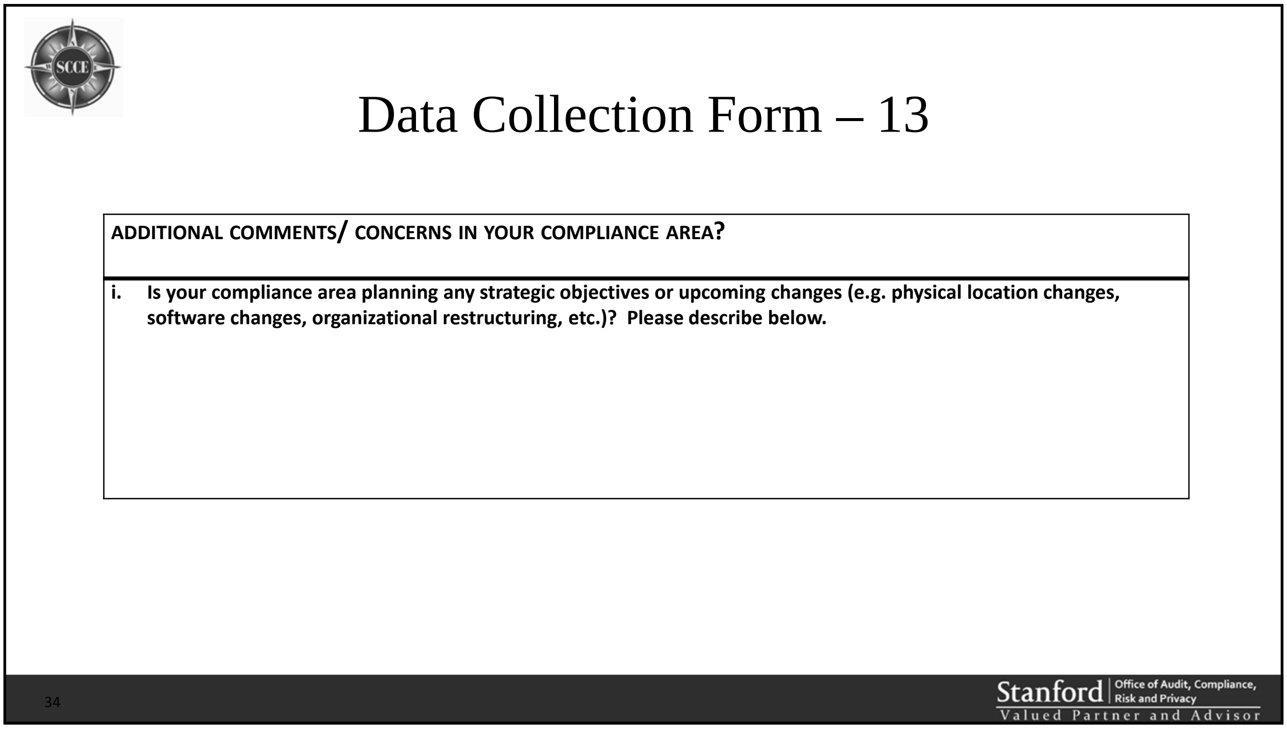
i. **Do P&P outline consequences for noncompliance with regulatory requirements and policies?**

7. **RESPONDING TO NONCOMPLIANCE AND MODIFYING THE PROGRAM AS NECESSARY**

i. **Has it been necessary to modify process or controls, or retrain individuals responsible, etc. to address non-compliance in the past year? If so, please explain.**

33

Stanford | Office of Audit, Compliance, Risk and Privacy
Valued Partner and Advisor



Data Collection Form – 13

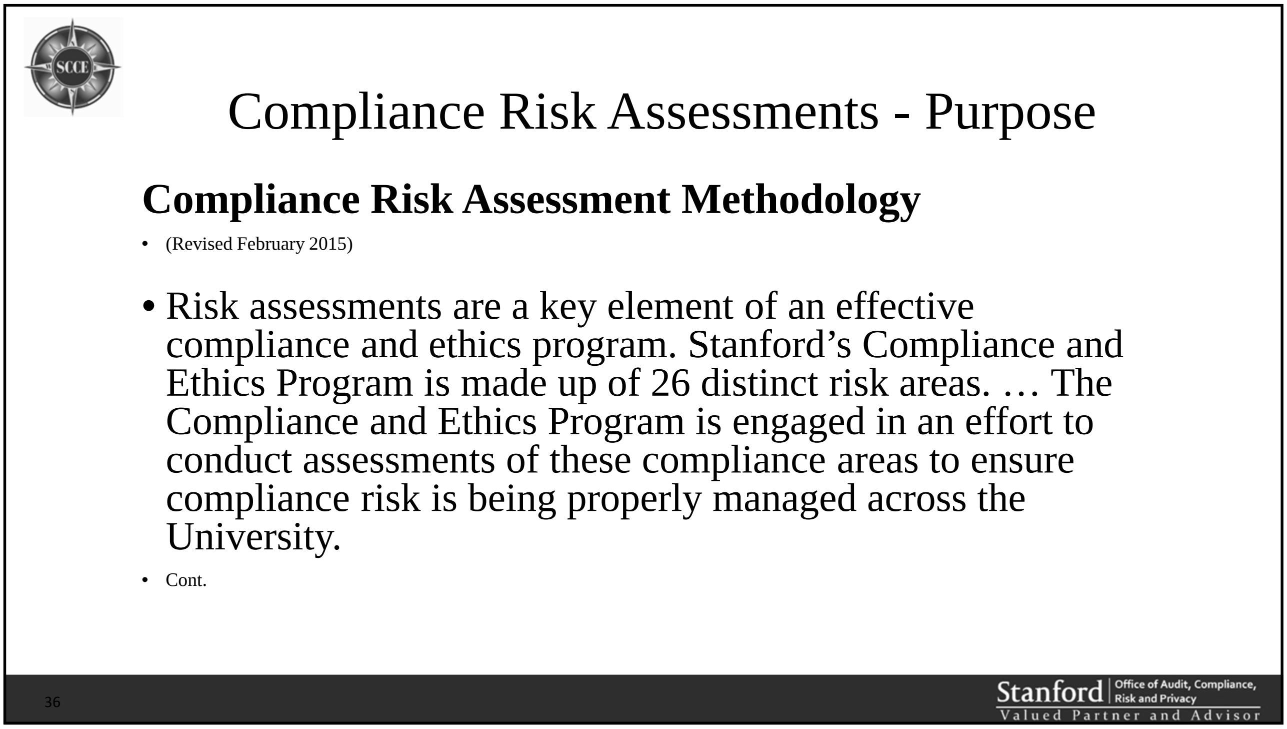
ADDITIONAL COMMENTS/ CONCERNS IN YOUR COMPLIANCE AREA?

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

34

Stanford | Office of Audit, Compliance, Risk and Privacy
Valued Partner and Advisor

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.

- Cont.

Compliance Risk Assessment (CRA) - Template

Compliance Risk Assessment

Executive Summary

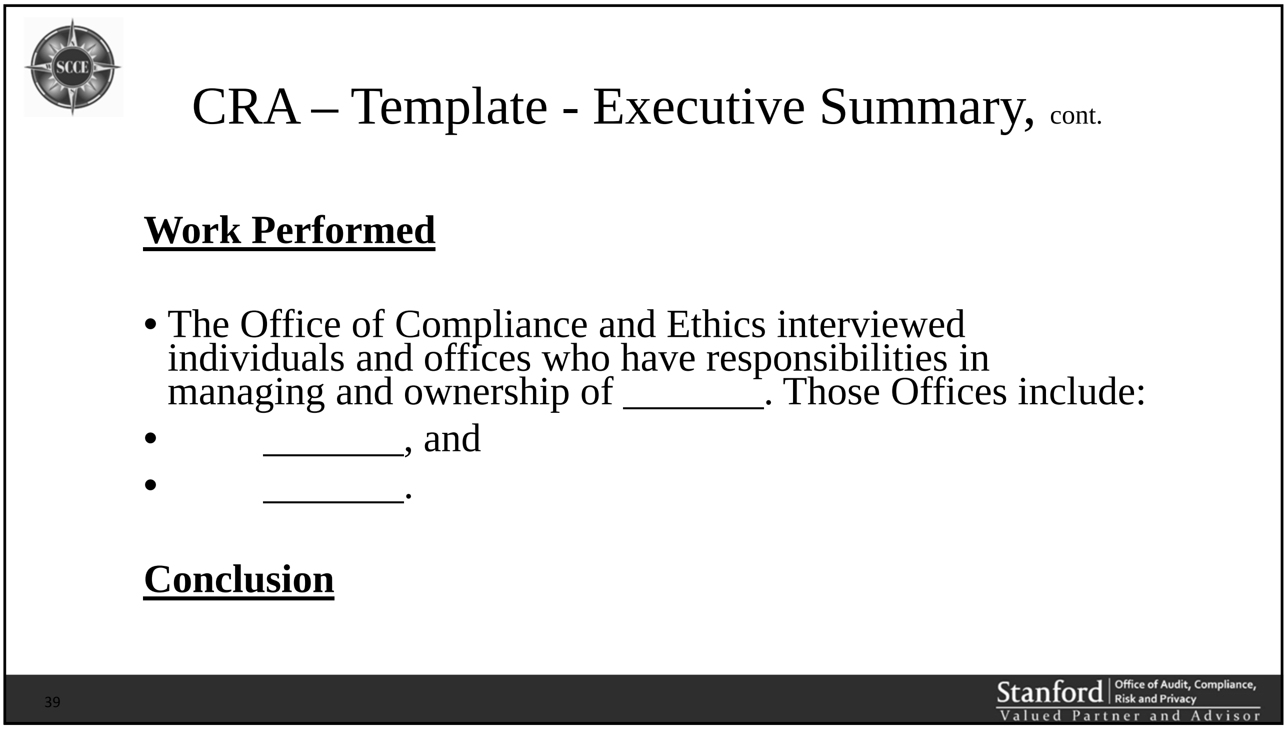
- **Introduction**
- **Background**
- Regulations regarding ________ and related matters are listed in **Attachment A**.

CRA – Template - Executive Summary, cont.

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.

	Sub Risk	**Reviewed on Attachment:**
1	Sub Risk 1	Attachment C
2	Sub Risk 2	Attachment D

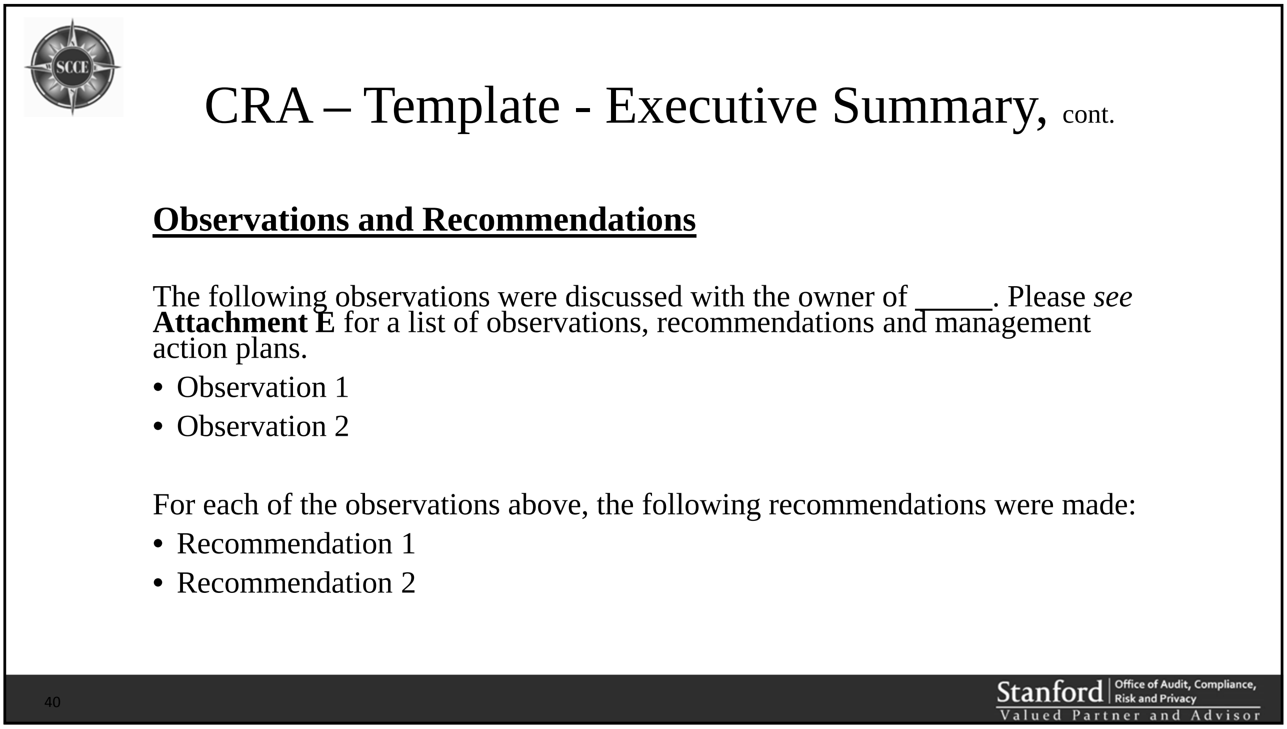


CRA – Template - Executive Summary, cont.

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



CRA – Template - Executive Summary, cont.

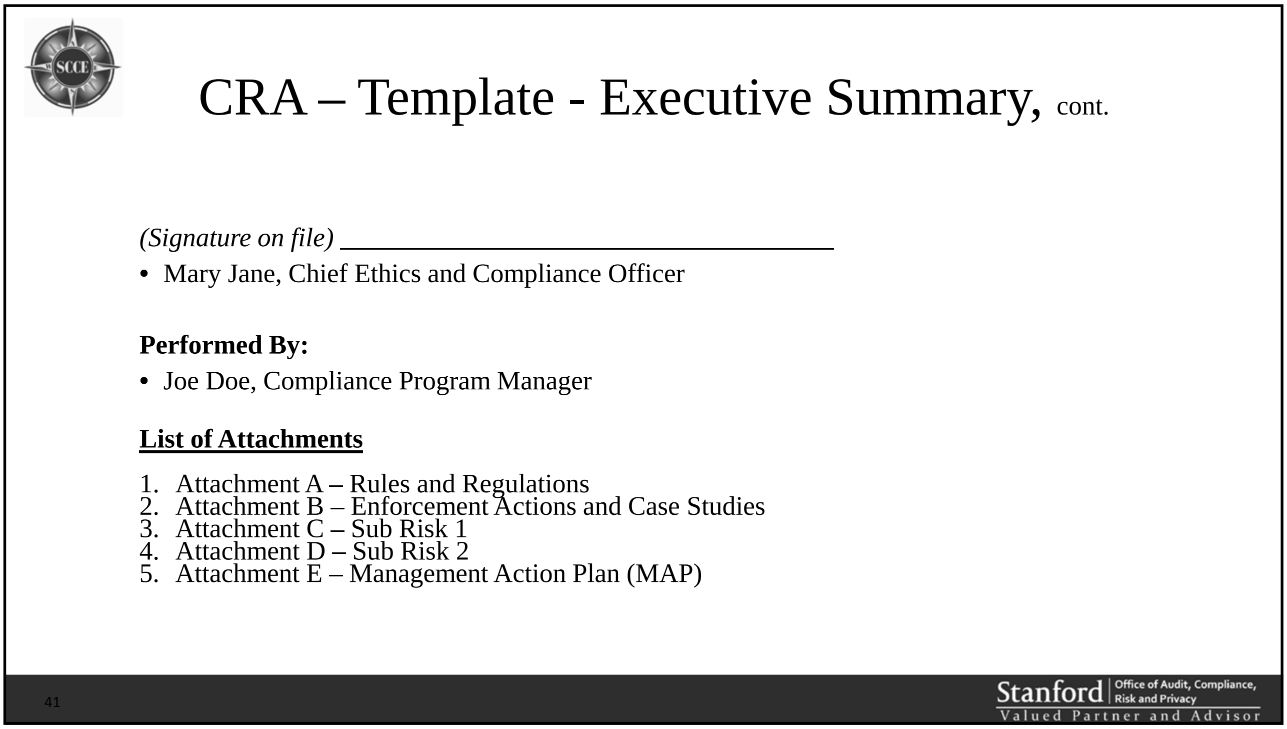
Observations and Recommendations

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



CRA – Template - Executive Summary, cont.

(Signature on file) ______________________________________

- Mary Jane, Chief Ethics and Compliance Officer

Performed By:

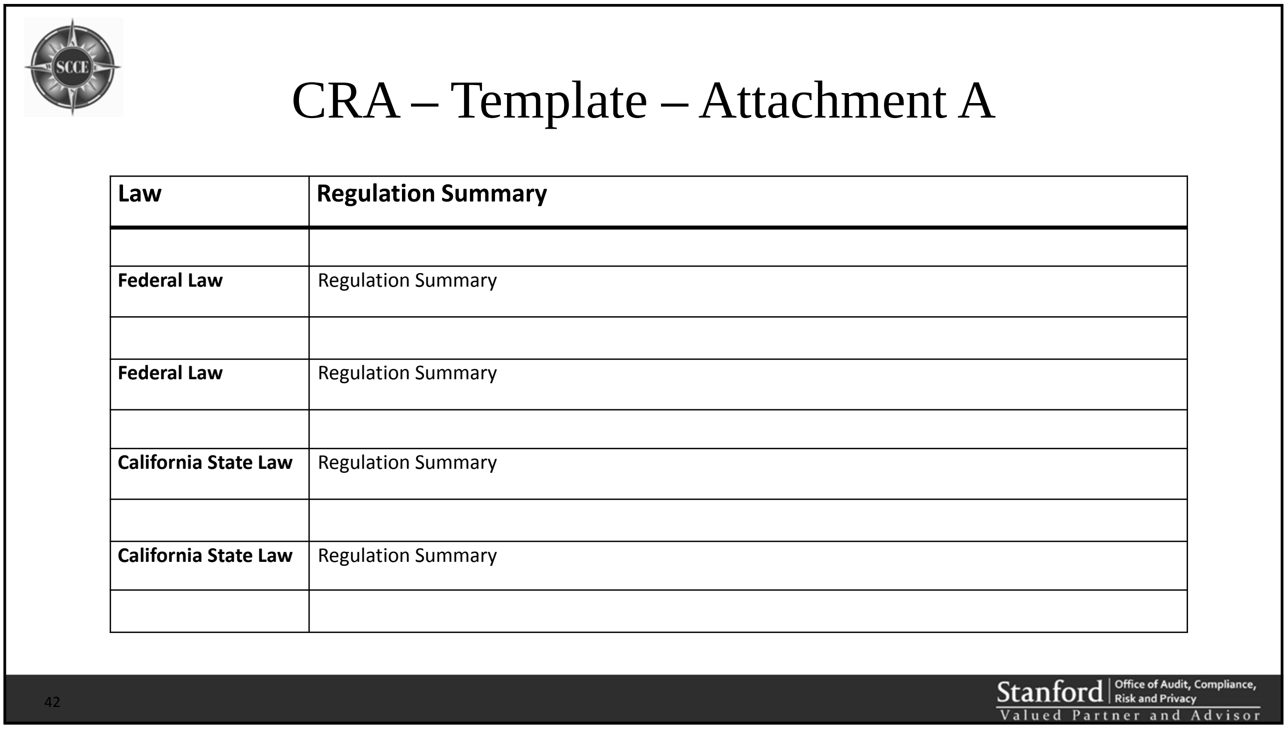
- Joe Doe, Compliance Program Manager

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)

41

Stanford | Office of Audit, Compliance, Risk and Privacy
Valued Partner and Advisor

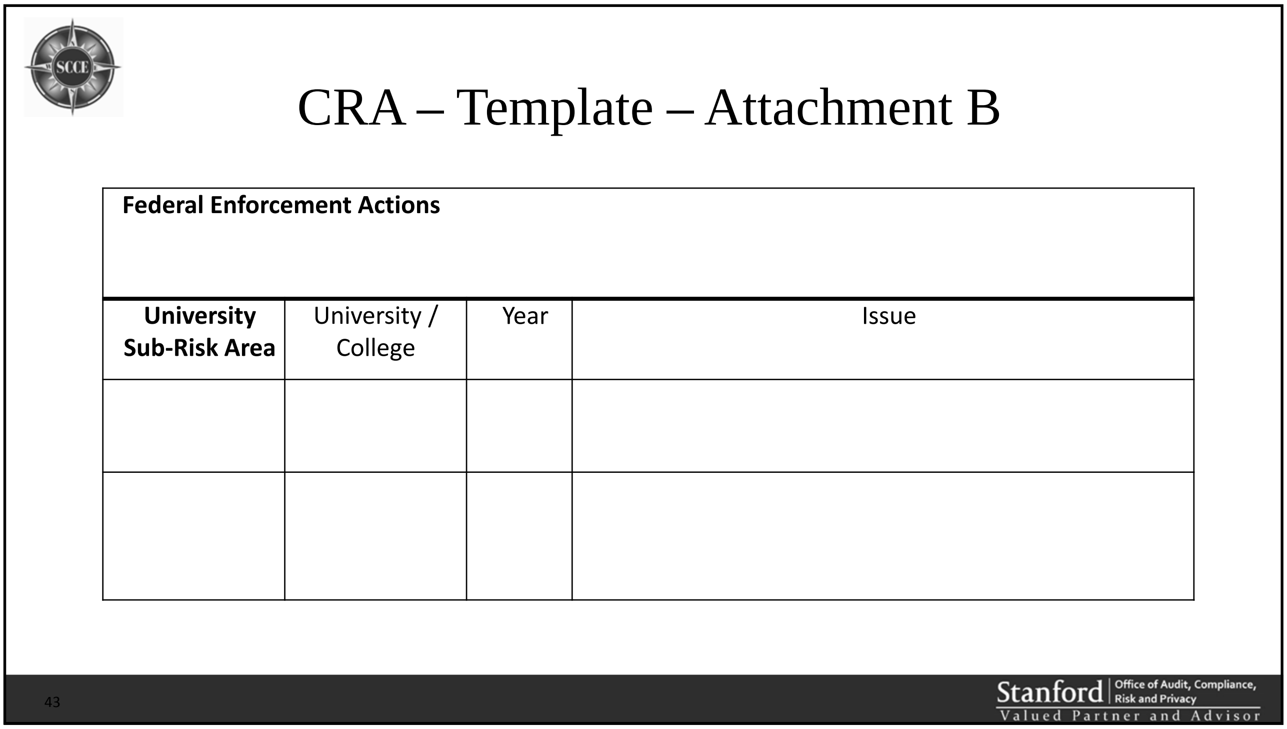


CRA – Template – Attachment A

Law	Regulation Summary
Federal Law	Regulation Summary
Federal Law	Regulation Summary
California State Law	Regulation Summary
California State Law	Regulation Summary

42

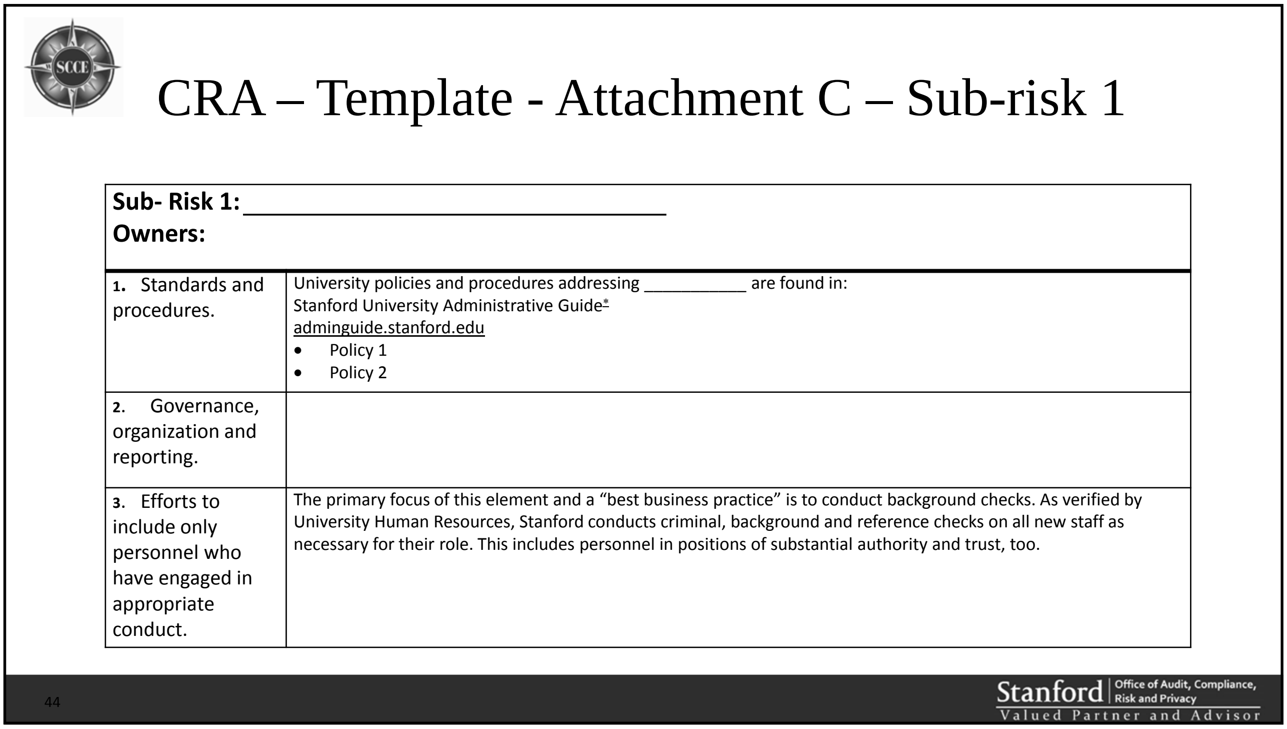
Stanford | Office of Audit, Compliance, Risk and Privacy
Valued Partner and Advisor



CRA – Template – Attachment B

Federal Enforcement Actions

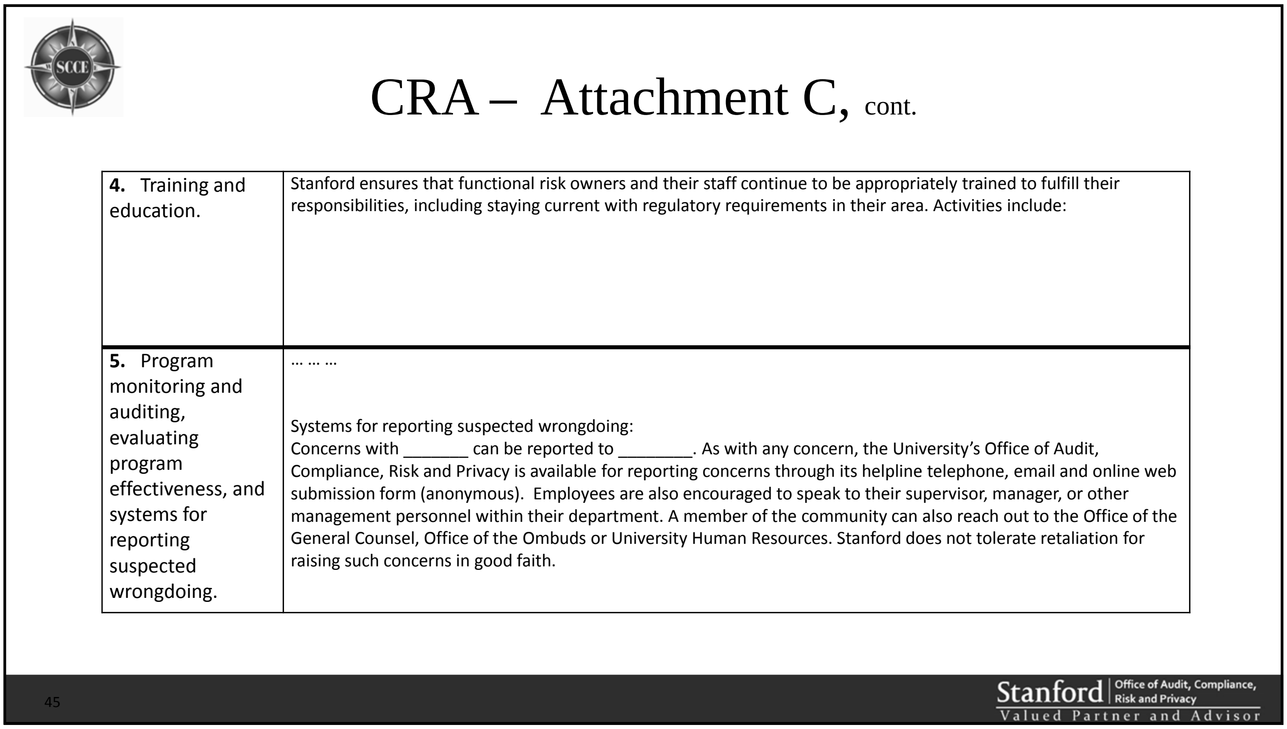
University Sub-Risk Area	University / College	Year	Issue



CRA – Template - Attachment C – Sub-risk 1

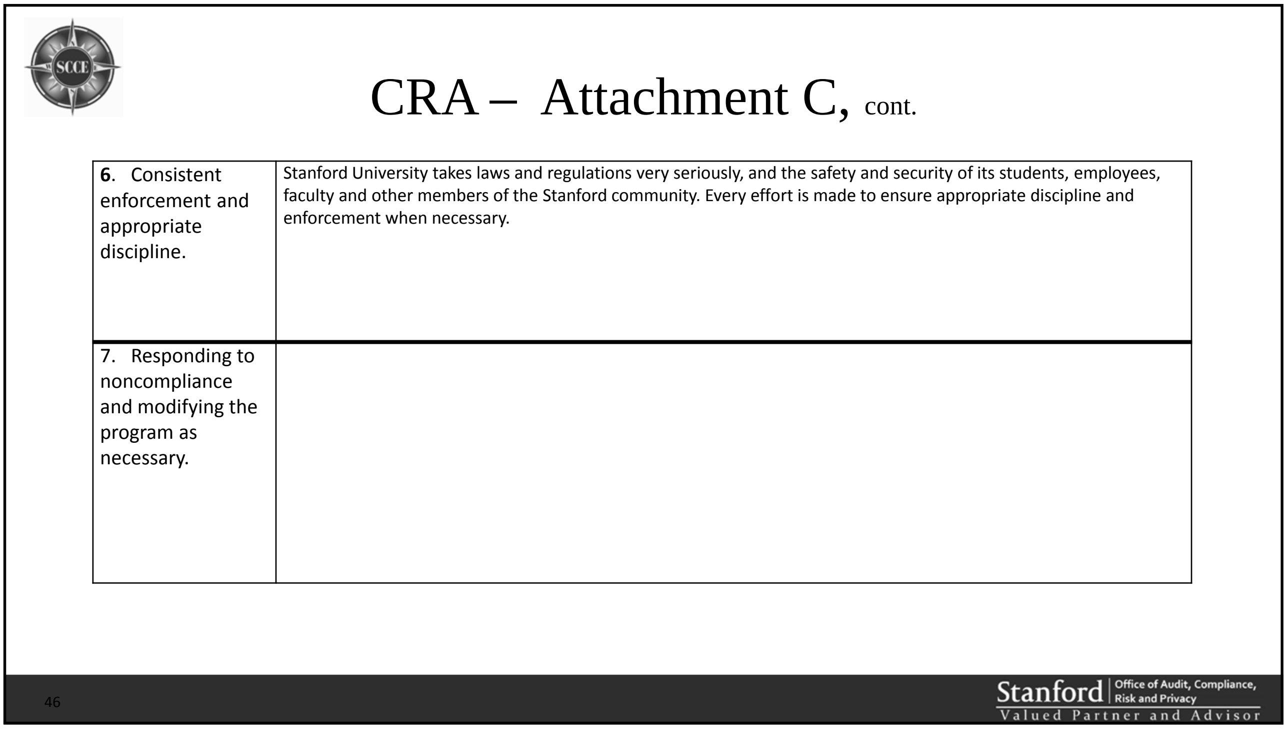
Sub- Risk 1:__________________________________
Owners:

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.	
3. Efforts to include only personnel who have engaged in appropriate conduct.	The primary focus of this element and a "best business practice" is to conduct background checks. As verified by University Human Resources, Stanford conducts criminal, background and reference checks on all new staff as necessary for their role. This includes personnel in positions of substantial authority and trust, too.



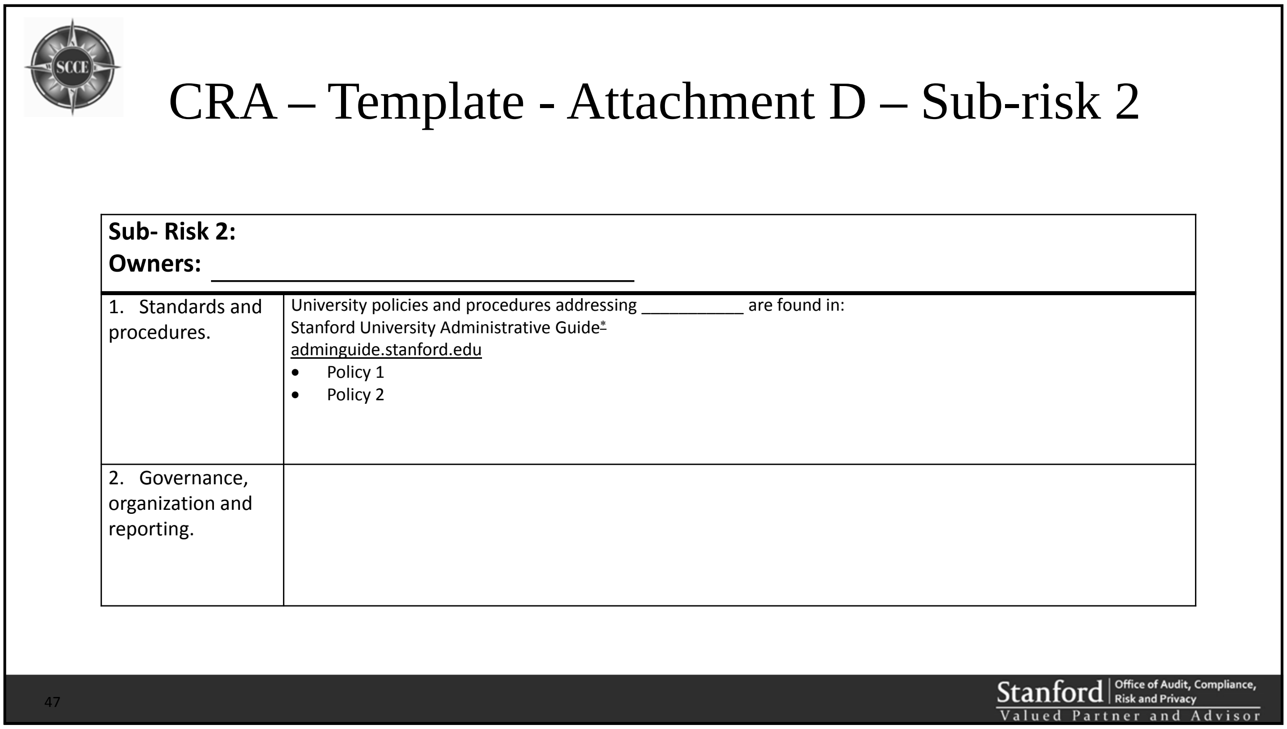
CRA – Attachment C, cont.

4. 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:
5. Program monitoring and auditing, evaluating program effectiveness, and systems for reporting suspected wrongdoing.	… … … Systems for reporting suspected wrongdoing: Concerns with _______ can be reported to ________. As with any concern, the University's Office of Audit, Compliance, Risk and Privacy is available for reporting concerns through its helpline telephone, email and online web submission form (anonymous). Employees are also encouraged to speak to their supervisor, manager, or other management personnel within their department. A member of the community can also reach out to the Office of the General Counsel, Office of the Ombuds or University Human Resources. Stanford does not tolerate retaliation for raising such concerns in good faith.



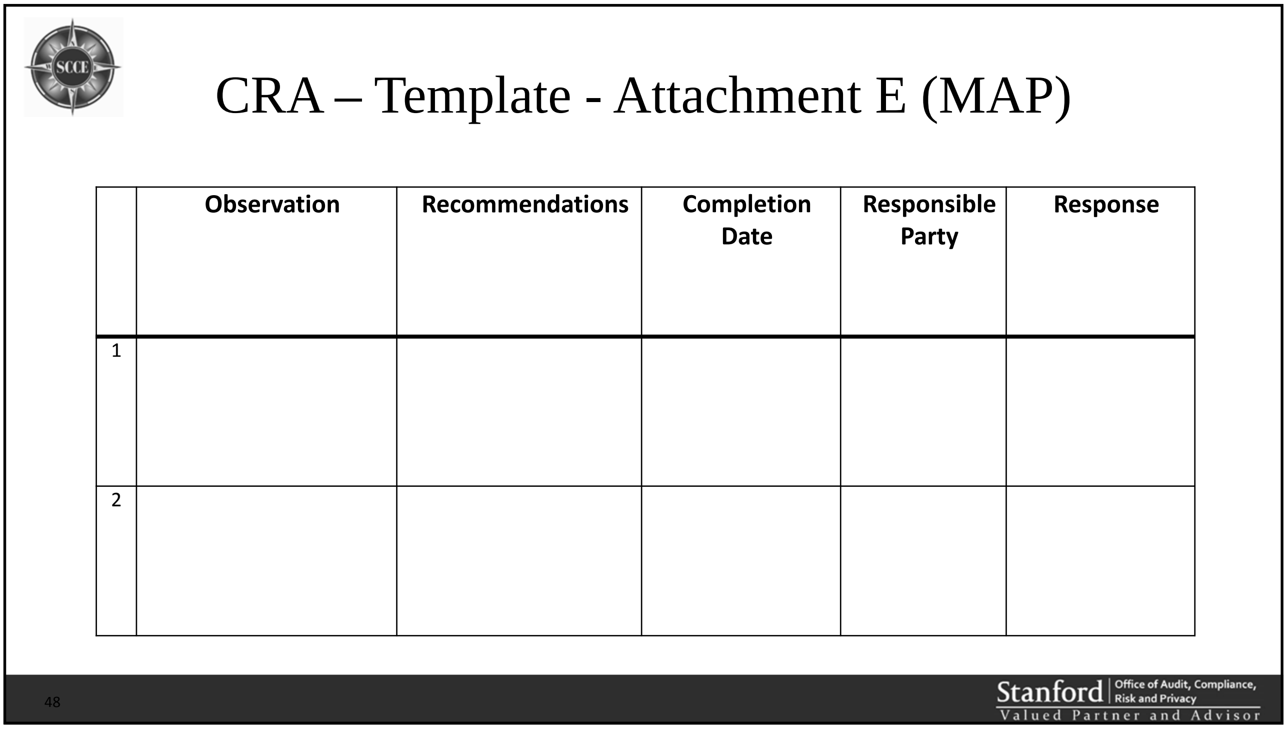
CRA – Attachment C, cont.

6. Consistent enforcement and appropriate discipline.	Stanford University takes laws and regulations very seriously, and the safety and security of its students, employees, faculty and other members of the Stanford community. Every effort is made to ensure appropriate discipline and enforcement when necessary.
7. Responding to noncompliance and modifying the program as necessary.	



CRA – Template - Attachment D – Sub-risk 2

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)

	Observation	Recommendations	Completion Date	Responsible Party	Response
1					
2					

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