Attachment I: QUICK REFERENCE

Institutional Compliance
Risk Assessment Matrix

Purpose of Initial Risk Assessment

Primary:
- To identify those compliance issues that have significant impact at the institutional level, including those risks that you feel are being adequately controlled. These are the areas that provide the infrastructure for the development of the compliance program.

Secondary:
- To identify compliance issues at every level of the institutional organization.
- To determine at each level those issues that are significant for that level.

Goal of This Risk Assessment

To populate the "Risk Assessment Matrix"

Required Resources

- All policies, procedures, rules and regulations that apply to the functions, processes and activities associated with the area of compliance.
- Ideally, employees with direct knowledge of the work being performed participate in a brainstorming session to identify risks that affect the successful achievement of the goals and objectives of the work unit.
- Recommended brainstorming question:

  "What are the problems you recognize, concerns you have, and risks you perceive regarding compliance with the federal and state laws and regulations, and the UH System/UHD policies and procedures in this work unit?"
- "Compliance Sections/Risk Assessments" required by UH System [Note: Included in this package. You are not limited to these compliance sections/risk assessments; however, these are required to be addressed in your assessment.]

Summary of Steps in the Risk Assessment Process (Detail Information Included in this Package)

Step 1: Identify the Compliance Risk and Exposure
- Develop a list of all the compliance risks that can affect the successful achievement of the work unit's goals and objectives.
- Determine the applicable law, rule, regulation, policy or procedure driving the risk.

Step 2: Measure the Compliance Risk
- The *Impact* of the risk, when it happens, on the achievement of the work unit goals and objectives. (High, Medium or Low)
- The *Probability* of the risk becoming a reality (High, Medium or Low)

Step 3: Prioritize the Compliance Risk
- Based upon their combined measurement of probability of becoming reality and the impact that would have on the work unit.
- All risk that have an *HH* "measurement value" would be placed at the top of the risk inventory, followed by *HM, HL, MH, MM, ML, LH, LM*, and *LL* groups in that order.
- Rank order each "measurement value" group from most to least significant via paired elimination.

Step 4: Populate the Risk Assessment Matrix (For Each "Measurement Value")
- Phase I – Compliance Section, Assessment Date, Sub-Section, Prepared By, Objective/Activity, Risk & Exposure, Potential Impact, Probability of Occurrence and Rank Before Controls.
- Phase II – Assign the "Responsible Party" (see requirements in this package). Specify the Operating and Oversight Controls. Assess the Rank After Controls (High, Medium or Low).

Step 5: Initial Review

Provide a copy of the Risk Assessment Matrix package to _____ on of before _____.

Resource: Effective Compliance Systems: A Practical Guide for Educational Institutions by David B. Crawford, Charles G. Chaffin and Scott Scarborough

QUICK REFERENCE

Risk Assessment Matrix (Without Monitoring Controls)

Compliance Section: (1) Responsible Party: (2) Assessment Date: (3)

Sub-Section: (4) Prepared By: (5)

Potential Impact

H – High Impact (If the risk happens, we will probably not achieve our objective or to do so will require major damage control)
M – Medium Impact (If the risk happens, we will have to do extra work or we will be inefficient, but we can still achieve our goal and objective)
L – Low Impact (If the risk happens, we will be aware of it but it will have little or no effect upon operations or the achievement of the objective)

Probability of Occurrence

H – High Probability (It will happen often)
M – Medium Probability (It is likely to happen but not often)
L – Low Probability (It is unlikely to happen at all)

Objective/Activity	Risk &Exposure	Potential Impact	Probability of Occurrence	Rank Before Controls	Operating Controls	Oversight Controls	Rank After Controls High Medium Low	Mitigation Strategy	
								Accept	Improve
(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	☐	☐
								☐	☐
								☐	☐
								☐	☐
								☐	☐

Identifying the Compliance Risk

- Required Resource - An inventory of all the policies, procedures, rules and regulations that apply to the work unit.
- The development of a list of compliance risk for the work unit is best achieved through brainstorming.
  - The Question:

    "What are the problems you recognize, concerns you have, and risk you perceive regarding compliance with the federal and state laws and regulations, and the UH System/UHD policies and procedures in this work unit?"

Resource: Effective Compliance Systems: A Practical Guide for Educational Institutions by David B. Crawford, Charles G. Chaffin and Scott Scarborough

QUICK REFERENCE

Populating the Risk Assessment Matrix

Item	Phase I	Phase II
(1) Compliance Section	See APPENDIX A • You are not limited to "only" theses categories, but you are required to either use the category or indicate "Not Applicable" for the Compliance Section listed.	*[Note: Typically assigned by the Compliance Officer/Committee.]*
(2) Responsible Party	-	See APPENDIX B • The ***one*** employee (management, faculty, or staff) who is responsible for the management of a particular compliance risk or risk area.
(3) Assessment Date	Current Date	-
(4) Sub-Section	The applicable Work Unit - A "work unit" is defined as the lowest level of budgeting within the organization. Any manager who has authority over and is responsible for a budget is the head of a work unit.	-
(5) Prepared By	Self Explanatory	-
(6) Objective /Activity	The applicable law, rule or regulation, or policy and procedure.	-
(7) Risk & Exposure	The specific risk identified and the exposure created if identified.	-
(8) Potential Impact	See APPENDIX C • The ***Impact*** of the risk, when it happens, on the achievement of the work unit goals and objectives. - High Impact – If the risk happens, we will probably not achieve our objective or to do so will require major damage control. - Medium Impact – If the risk happens, we will have to do extra work or we will be inefficient, but we can still achieve our goals and objectives. - Low Impact – If the risk happens, we will be aware of it, but it will have little or no effect upon operations or the achievement of the objective.	-

Resource: Effective Compliance Systems: A Practical Guide for Educational Institutions by David B. Crawford, Charles G. Chaffin and Scott Scarborough

Item	Phase I	Phase II
(9) Probability of Occurrence	See APPENDIX C • The ***Probability*** of the risk becoming a reality. - High Probability – It will happen often. - Medium Probability – It is likely to happen, but not often. - Low Probability – It is unlikely to happen at all.	-
(10) Rank Before Controls	See APPENDIX C Prioritization is simply ranking the risk based upon their combined measurement of probability of becoming reality and the impact that would have on the work unit. • All risk that have an *HH* measurement value would be placed at the top of the risk inventory, followed by *HM, HL, MH, MM, ML, LH, LM*, and *LL* groups in that order. • Prioritize each measurement combination separately by using a "paired elimination" method. [Note: For example, consider the entire *HH* group. Decide on the most significant risk from this group and the least significant risk from this group. Place the two at the top and bottom respectively on a new ranked *HH* list and remove these two from the unranked *HH* list. Continue the process until all items have been transferred to the ranked *HH* list.]	-

Item	Phase I	Phase II
(11) Operating Controls	-	• Operating Controls – Those procedures that are applied day-to-day by operating staff to every event/transaction in a process at the time of its creation (real time) to ensure compliance with the policies and procedures governing the process. In summary, these execution controls are: - Embedded in day-to-day operations ▫ Policies and procedures ▫ Segregation of duties ▫ Reconciliation/comparison - Performed on every event/transaction - Performed by the generators of the event/transaction - Performed in "real time," as the event/transaction is executed
(12) Oversight Controls	-	• Oversight Controls ***(for "A List Risk"- i.e. Risk with HH and HM Measurement Values)*** – Those procedures applied by middle and senior management soon after an event/transaction has occurred to ensure that supervisory controls have been applied as designed, including review of status reports, exception reports, actual versus planned analysis, etc. In summary, these executive controls are: - Exception reports, status reports, analytical reviews, variance analysis - Performed by representatives of executive management - Performed on information provided by supervisory management - Performed within a short period (Weeks/months) after the event/transaction is originated
(13) Rank After Controls	-	Prioritize the inventory into: • High Risk (Risks that need to be constantly managed), • Medium Risk (Risks that need to be monitored), and • Low Risk (Risk that can usually be accepted).

APPENDIX A

Compliance Sections/ Risk Assessments

Academic Affairs
- Institutional Accreditation
- Institutional Accreditation
- THECB Reporting - Inst. Data
- THECB Requirements – Academic Degree Program

Advancement
- Gift Receipting - IRS Guidelines
- State / Federal Reports of Foreign Gifts

Contract Administration
- BOR Approvals
- Delegation of Authority
- Competitive Procurement Requirements (See Purchasing)
- Consulting and Professional Service Agreements
- Major Information System Agreements
- Contract Reporting
- OGC Review and Approval

Environmental Health and Safety
- Radiation Safety – Material
- Radiation Safety – Waste
- Laser Safety
- Controlled Substances and Dangerous Drugs
- Biosafety - Committee (NIH Requirements)
- Biosafety - Listed Agents
- Lab Registration - Select Age
- Public Health and Bioterrorism Preparedness / Response Act
- Chemical Safety - TDH Hazardous Communication Standards
- Chemical Safety - Tier II Chemical Inventory and Reporting
- Chemical Safety - Lab Safety Program
- Waste Management - Hazardous and Industrial Solid Waste Regulations
- Waste Management - Biological Waste
- Waste Management - General Refuse and Trash
- Waste Management - Recycle / Pollution Prevention Efforts
- Waste Management - Grease / Lint Traps
- Water Pollution - Spill Prevention Control and Countermeasure
- Water Pollution - Clean Water Act
- Water Pollution - Above Ground and Underground Storage Tanks
- Air Emissions - Annual Emissions Inventory
- Air Emissions - Air Permit Requirements
- Air Emissions - Stage II Vapor Recovery Rules
- Air Emissions - Permit by Rule for Specific Campus Units
- Air Emissions - Refrigerant Use / Recovery Rules
- Air Emissions - Regional Air Rules
- Fire and Life Safety - Inspections, Testing and Maintenance (Sprinkler Systems, Stand Pipe and Hose Systems; Private Fire Service Main, Fire Pumps, Water Storage Tanks)Storage Tanks)

Facilities
- Contract Reporting
- Chemical Safety
- Utility Services - State Facility Energy Management Program
- Utility Services - State Boiler Inspection Compliance Items

Finances
- Tax - Preparing and Filing Required Tax Forms
- Tax - Miscellaneous Tax Compliance Areas

Financial Aid

Health Care Billing and Confidentiality
- Confidentiality - Medical Records

Human Resources
- Family and Medical Leave Act
- Tax Deferred Annuities - Excess Contributions
- Pay Guidelines for Staff Employees
- Classification of Staff Jobs
- Security Sensitive Positions
- Recruitment of Postings and Selection of Staff
- Employment of Foreign Nationals
- Discipline / Dismissal of Staff Employees

APPENDIX A

Compliance Sections (cont'.)

Information Technology

Law - OAA/EEO

- Annual Affirmative Action Plan
- Annual Veterans Report
- Equity in Athletics Disclosure Report
- Texas Labor Code - Vets Quarterly Report
- Texas Labor Code - EEO Annual Report
- Texas Labor Code - Minority Hiring Annual Report
- Texas Labor Code - Discrimination Training
- Integrated Postsecondary Education Data System
- Texas Plan Reports - UH System Governing Board
- Texas Plan Reports - UH System Employees
- Texas Plan Reports - UH Faculty

Law Enforcement

- Vehicle Use Reports
- Record Retention
- Annual Vehicle Registration / Inspection
- Disclosure of Crimes and Crime Prevention Programs
- Required Reporting of Juveniles in Lockup
- Separation of Juveniles by Sight and Sound from Adults
- Reporting of Seized and Forfeited Property
- Required Continuing Education
- Telecommunications Operator Training

Purchasing

- Competitive Procurement Requirements
- Tx Gov. Code 2155.138, Purchases from People with Disabilities
- Tx Gov. Code 2155.441, Purchases from People with Mental Retardation / Physical Disabilities

Sponsored Research

- OMB Circular A-110 - General Requirements
- OMB Circular A-110 - Specific Requirements
- OMB Circular A-133
- Use of Animals in Research
- Lobbying (Bryd Amendment)
- Human Subjects Compliance
- Education in Use of Human Subjects (NIH)
- Recombinant DNA
- Misconduct in Science
- Procurement Integrity
- Buy American Act
- Fly American Act
- Acknowledgement of Federal Support
- Federal Debt Delinquency
- Conflict of Interest (NSF & PHS)
- Rights to Inventions (Bayh - Dole)
- PHS Salary Cap
- Public Health and Bioterrorism Preparedness / Response Act
- OMB Circular A-21, Cost Accounting Standards - General Requirements
- OMB Circular A-21, Cost Accounting Standards - Specific Requirements

APPENDIX B

Responsible Party

Accountability is a consistent theme throughout an effective institutional Compliance program. Accountability presumes ***exclusive responsibility***. An acceptable "responsible party" must exhibit each of the following characteristics:

- Exclusive responsibility for managing the risk,
- Appropriate knowledge to manage the risk, and
- Necessary authority to manage the risk.

Exclusive Responsibility

The purpose of exclusive responsibility is to ensure accountability. There must be no opportunity for passing the buck or pointing fingers. If the responsible party identification process for a risk seems to logically or inevitably produce more than one individual, one of two situations exists:

1. The "A" list risk is actually two or more separate risks and should be reanalyzed, separated and assessed to determine if each one is an "A" list risk.
2. One or more of the identified responsible parties lack appropriate knowledge or authority to manage the risk. The individual with the authority to allocate resources and take corrective actions to ensure effective management of the risk is the "responsible party".

Responsible parties with both the knowledge and authority to manage the risk may delegate the responsibility to a subordinate either on the basis of lack of time to devote to the program or lack of detailed knowledge about the day-to-day activities associated with the risk. The issue is not delegation of work, but rather, the delegation of responsibility and accountability. ***The responsible party cannot delegate responsibility or accountability for the management of their assigned risk.***

Appropriate Knowledge to Manage the Risk

The responsible party must have an appropriate level of knowledge about the risk area to make decisions regarding the allocation of resources and the design of mitigation strategies to manage the risk. **This does not imply**:

- Knowledge of detailed, day-to-day activities for managing the risk, or
- The personal performance of the monitoring controls needed to identify potential instances of noncompliance.

"Appropriate level of knowledge" does imply that the responsible party has line management access to detailed knowledge relating to the risk being managed.

Necessary Authority to Manage the Risk

The responsible party must have the authority to allocate resources and take corrective action to ensure effective management of the risk in question.

Designation of the responsible party for each risk is one of the most critical tasks in the compliance program. These are the players who will be the backbone of the compliance program. This list of individuals must be reviewed and approved by the chief executive officer.

Resource: Effective Compliance Systems: A Practical Guide for Educational Institutions by David B. Crawford, Charles G. Chaffin and Scott Scarborough

APPENDIX C

Measuring and Prioritizing the Compliance Risk

Measuring the Compliance Risk

The ***Impact*** of the risk, when it happens, on the achievement of the work unit goals and objectives.

- High Impact – If the risk happens, we will probably not achieve our objective or to do so will require major damage control.
- Medium Impact – If the risk happens, we will have to do extra work or we will be inefficient, but we can still achieve our goals and objectives.
- Low Impact – If the risk happens, we will be aware of it, but it will have little or no effect upon operations or the achievement of the objective.

The ***Probability*** of the risk becoming a reality.

- High Probability – It will happen often.
- Medium Probability – It is likely to happen, but not often.
- Low Probability – It is unlikely to happen at all.

Figure 1: Risk Measurement Combinations

Likelihood ? / Impact ?	**High**	**Medium**	**Low**
High	Extensive Risk Management Required	Considerable Risk Management Required	Manage & Monitor Risk
Medium	Manage & Monitor Risk	Manage & Monitor or only Monitor Risk	Monitor
Low	Monitor	Monitor or Accept Risk	Accept Risk

Extensive Risk Management = All local operating controls and traditional in-depth audit
Considerable Risk Management = All local operating controls and traditional auditing work
Manage and Monitor = All local operating controls
Monitor = Operating controls and monitoring controls from local operating controls
Accept = No local operating controls

Prioritizing the Compliance Risk

Prioritization is simply ranking the risks based upon their combined measurement of probability of becoming reality and the impact that would have on the work unit.

- All risk that have an *HH* measurement value would be placed at the top of the risk inventory, followed by *HM, HL, MH, MM, ML, LH, LM*, and *LL* groups in that order.
- Prioritize each measurement combination separately by using a "paired elimination" method. [Note: For example, consider the entire *HH* group. Decide on the most significant risk from this group and the least significant risk from this group. Place the two at the top and bottom respectively on a new ranked *HH* list and remove these two from the unranked *HH* list. Continue the process until all items have been transferred to the ranked *HH* list.]

Populating the Compliance Risk Matrix

The Compliance Risk Assessment Matrix is a simple, direct way to report the work unit's compliance risk assessment to the compliance officer. Please note:

All identified risks that remain after the identification, measurement, and prioritization phase should be reported on the matrix.

A single Risk Assessment Matrix should be completed for each measurement value, i.e., one for *HH* by paired elimination rank, one for *HM* by paired elimination rank, etc.

Resource: Effective Compliance Systems: A Practical Guide for Educational Institutions by David B. Crawford, Charles G. Chaffin and Scott Scarborough