# 04A. RISK MANAGEMENT: HOW TO MAKE IT PART OF YOUR STRATEGY

November 6 – 8, 2013

**Shulamith Klein**
Chief Risk Officer
Emory University – Emory Healthcare

## I. ERM ANNUAL PROCESS

| **Risk Identification** June - July | **Risk Management Plans** August - September | **Risk Hearings** October - June | **Monitoring and Evaluation** (Ongoing) |
|---|---|---|---|
| • Steering Comm identifies risks for major operational areas<br>• Risks ranked by frequency and severity<br>• "Top 50", based on decreasing risk factors, are designated "Key Risks"<br>• Committee identifies individuals responsible for overseeing management of each key risk ("Risk Management Process Owner")<br>• Key Risks reviewed with Exec Comm | • President charges Risk Management Process Owners with preparing two-page plan in 60 days<br>• Plans include detailed description of risk, risk components, steps being taken to manage the risk, operational and communication responses to adverse occurrences<br>• Plans must clearly identify who is responsible and accountable for specific actions<br>• Steering Comm reviews Risk Management Plans<br>• Risk Management Process Owners revise plans based on Steering Comm feedback<br>• Risk Management Plans go to Exec Comm | • Risk Management Process Owners present to Exec Comm<br>• Five risk hearings, three hours each<br>• Process Owners provide five -minute overview of each risk, followed by five minutes Q&A<br>• Exec Comm probes for potential gaps between the risk and the response plan<br>• Process Owners may be asked to return with additional information at the next hearing<br>• Participants identify "best practices"<br>• Executive Session includes overview of total risk for specific operational area and ERM process overall | • Key Risks and specific Risk Management Plans are reviewed throughout the year<br>• Relative frequency and severity may be adjusted resulting in the addition or deletion of key risks<br>• Updates to Risk Management Plans are requested as needed |

## II. RISK FACTOR FREQUENCY

| Risk factor = (frequency /2) + severity |
|---|

### A. Frequency (likelihood of occurring)

1 - low: <10% chance of occurring in 2 years

2 - medium: ≥10% but <25% chance of occurring in 2 years

3 - high: ≥25% but <50% chance of occurring in 2 years

4 - very high: ≥50% chance of occurring in 2 years or already occurring

### B. Severity (potential impact)

1 - minor: unlikely to have permanent or significant effect on institution's reputation or achievement of its strategic objectives

2 - moderate: will have significant impact on institution but can be managed without major impact

3 - serious: will have significant effect on institution and require major effort to manage and resolve occurrence, as well as its ramifications

4 - very serious: will threaten existence of institution if not resolved

## III. Sample Template Used to Track Key Risks

| Code | Risk | Freq | Sev | Risk Factor | RMPO | POL | Steering Committee Chair |
|---|---|---|---|---|---|---|---|
| CSP2 | Fire in a facility | 3 | 2 | (3/2) +2 = 3.5 | Watson | Early | Early |
| IT1 | Breach of computer security/ confidentiality | 4 | 2 | (4/2) +2 = 4 | Sanford | Mendola | Mendola |

**Note**: Actual data is maintained in Excel. For conference purposes, this handout is in Word format.

**Code**: risks are grouped by operational area; "CSP2" is the 2nd key risk in the queue for Campus Safety & Physical Plant; "IT1" is 1st key risk in the queue for IT, etc.

**Risk**: one-line description of the specific risk

**Frequency**: likelihood of occurrence within two years (refer to Frequency & Severity Rating chart)

**Severity**: impact on organization's ability to conduct business as usual (refer to Frequency & Severity Rating chart)

**RMPO**: Risk Management Process Owner is the individual assigned responsibility for drafting the Risk Management Plan and keeping it current. The RMPO is not necessarily the individual with primary operational responsibility for managing the risk, but must be sufficiently familiar with the risk to prepare a coherent Risk Management Plan.

**POL**: Primary Operational Leader is the manager/executive with primary (but often not sole) operational responsibility over the functional area where the risk has the greatest potential impact.

**St Committee Chair**: The individual(s) who sits on the Steering Committee representing the respective operational area captured by the specific risk; "Early" is VP for Campus Services; "Mendola" is Chief Information Officer, etc.

## IV. ERM Risk Hearing

### A. ERM Risk Hearing Presentations to Executive Committee

*(One-slide PowerPoint for "new" risk not previously presented)*

Risk:

- Examples and/or components of the risk
- Steps currently in place to manage the risk
- Issues
- Proposed next steps (if needed)

### B. ERM Risk Hearing Presentations to Executive Committee

*(One-slide PowerPoint for "recurring risk" previously presented)*

Risk:

- Is there anything new to report about this risk over the past year?
- Occurrences of risk in the past year
- Lessons learned
- Proposed next steps (if needed)

## V. Sample resources


- Klein, Shulamith, Michael Mandl and Stephen Sencer. "Learning to Harmonize." *Business Officer Magazine.* NACUBO. December 2008.
- Stippich, Warren and Bailey Jordan. "Is ERM right for your organization?" *Corporate Governor*. Grant Thorton. Winter 2010.
- *Road to Implementation: Enterprise Risk Management for Colleges and Universities. 2009. Arthur J. Gallagher & Co.*
- http://f2.washington.edu/treasury/riskmgmt/home

# RISK ASSESSMENT AND MONITORING
# THE UNIVERSITY OF MINNESOTA'S EXPERIENCE

November 6 – 8, 2013

**Lynn A. Zentner, J.D.**
Director, Office of Institutional Compliance
University of Minnesota

## I. Introduction

Today's compliance environment is challenging. There are ever increasing regulatory requirements imposed on institutions of higher education. Examples include the Public Health Service's conflict of interest regulations (42 C.F.R. §50, Subpart F), effective August 25, 2011, with an implementation date of August 24, 2012, and the enhanced requirements under the HIPAA/HITECH ACT (45 C.F.R. §164), effective March 26, 2013, with an implementation date of September 23, 2013. Each required additional resources to achieve compliance and, going forward, require enhanced oversight to ensure an acceptable level of compliance. At the same time, resources are dwindling in higher education, particularly in the public sector. While it may seem that adding the burden of risk assessment in the context of the current environment is unwise, the effort in fact can instead achieve outcomes that provide opportunity for risk recalibration and the reallocation of resources. The following provides a road map for the process currently underway at the University of Minnesota. The last compliance-related risk assessment was conducted during the timeframe 2002-2005. We anticipate a more frequent implementation of the risk assessment process going forward than what has occurred historically but it will likely not be annually.

## II. The Nature of the University's Compliance Infrastructure

The University's Compliance Program ("the Program") is focused entirely on regulatory risk, in other words, compliance with federal, state, and local laws and University policy. Operational and strategic risk is the responsibility of the institution's leaders. The Program works through a network of approximately 30 compliance partners. Each reports to one of the University's Vice Presidents.

## III. Achieving Buy-In

In an era of dwindling resources, the first task was to convince senior leaders and the Compliance Partners of the value that would result from the effort. We were mindful of the infrastructure for effective compliance and ethics programs found in Chapter 8 of the Federal Sentencing Guidelines which requires a risk assessment component and expects that organizations will take the steps necessary to reduce risk based on the outcomes of the risk assessment process.

We began the initiative with senior leaders. The Program has always had a close relationship with the Office of the General Counsel and the Office of Internal Audit. Obtaining buy-in with the General Counsel and University Auditor was easily achieved. The next step was to persuade the Executive Oversight Compliance Committee (EOCC). This Committee consists of seven executives who meet regularly throughout the year to address compliance-related matters. In addition to the University Auditor and the General Counsel, the Committee is comprised of the Vice President for Research, the Dean of the Medical School and Vice President of the Academic Health Center, the Vice President for Human Resources, the Vice President for University Services and the Vice President for Equity and Diversity. While we readily acknowledged in our communications with these senior leaders the resources involved

in implementing the risk assessment process University-wide, we also emphasized the benefits, namely an opportunity to reallocate resources as appropriate, depending on the outcomes, and to re-evaluate the institution's appetite for risk. We ultimately achieved the buy-in.

The next step was to obtain the buy-in of the Compliance Partners. Since these individuals all reported to a member of the EOCC, and all of the members of the EOCC agreed to proceed with the risk assessment process, that effort was not particularly difficult but charting the course for the process required additional effort. Through dialogue and history regarding the Compliance Program, we achieved that buy-in. We met with the Compliance Partners as an entire group at least twice. During those meetings and conversations, we addressed the benefits that would accrue from the effort, how the effort aligned with the Board of Regents' Internal Control Policy, the scope of the risk assessments to be conducted, the spreadsheet that would be used for the process, how to rank each risk, what detail we expected, and the heat map format that would likely be used at the end of the process to chart the University's risk profile. We also discussed the step that would follow the risk assessment process, namely the implementation of monitoring processes to effectively evaluate, on an ongoing basis, the effectiveness of the University's operating controls and to detect problems. We ultimately achieved that buy-in as well.

## IV. The Process and Related Documents

### *A. The Legal Compliance Risk Assessment Form and Related Instructions*

The form has eight columns. We asked the Compliance Partners to use this form to:

- List key regulations or statutes governing their compliance risk areas and, in addition, provide lists of key provisions or categories of provisions depending on the comprehensiveness of the particular statute or regulation;
- List the legal or policy consequences for non-compliance;
- State whether the University has a corresponding administrative policy and, if so, state whether the policy requirements fail to meet, meet, or exceed statutory/regulatory requirements;
- State the level of impact (high, medium or low) that would result from non-compliance;
- State the probability of an occurrence (high, medium or low) reflecting non-compliance;
- State the total level of risk which is comprised of impact plus the likelihood of non-compliance;
- State whether the risk area is owned by more than one compliance partner;
- State whether there is an opportunity to reduce burden and still remain compliant.

See Spread Sheet titled 2013 Legal Compliance Risk Assessment, Attachment A. To accomplish this, we provided a set of instructions. See Instructions for the 2013 Legal Compliance Risk Assessment, Attachment B. Mindful of the issues of burden, we advised the Compliance Partners that, if they had already compiled this information recently in a different format, they would not be asked to repeat the process but could submit the alternate format to the Compliance Program.

### *B. Operationalizing the Process*

We defined the level of detail we expected the spreadsheet to reflect. If a statute or set of regulations had only a few requirements, we asked the Compliance Partners to list all of them. If, on the other hand, the regulations were very detailed, we asked them to list key provisions or

categories of provisions. The HIPAA HITECH regulations are an example of the latter. See Attachment C.

If a statute or set of regulations had a range of consequences for non-compliance, we asked the Compliance Partners to report the range of possibilities. If the statute or regulations provide no consequence for non-compliance, that information should also be reported.

To the extent that Compliance Partners determined that certain administrative policies exceeded regulatory requirements, we asked them to consider the rationale. The Compliance Office is playing no role in determining whether risk should be recalibrated in these circumstances but is simply asking Compliance Partners together with the Vice Presidents to whom they report to consider the justification.

In order to determine the level of impact, we referred the Compliance Partners to the document titled Legal Compliance Reporting Standards which is also used for the Legal Compliance Reporting Process described below. See Attachment D. The categories address the costs associated with responding to a compliance failure, the potential harm to individuals, reputational harm, adverse action by a regulatory body, whether a senior leader has been accused of misconduct, whether criminal charges could result, or whether the incident is minor in nature and/or reflects an isolated incident with few consequences.

With respect to the probability that a compliance-related incident will occur, we asked the Compliance Partners to use an approach developed by one of the University's Vice Presidents who described the three levels as follows:

- High: the probability that a compliance failure will typically occur multiple times a year;
- Medium: the probability that a compliance failure will occur once per year; and
- Low: the probability that an event will likely occur once every ten years.

Next, we asked the Compliance Partners to evaluate the "total level of risk" (impact plus likelihood of occurrence). There is no science to this aspect of the process. The significance of the impact may be medium but the likelihood of occurrence may be low. Whether the composite assessment will be "medium" or "low" is a decision to be made by the Compliance Partner in conjunction with the responsible vice president.

Where a compliance risk area has more than one "owner", we asked the Compliance Partners to look carefully at issues involving duplication of effort as well as gaps. Either can occur in these circumstances. Ultimately, having a list of units that share responsibility for a given regulation will be useful to aid in the coordination of compliance efforts, avoid possible duplication, and also close any gaps that may exist.

Finally, we asked the Compliance Partners to look carefully at opportunities to reduce burden and still be compliant. We provided an example of a recent risk recalibration effort that was initiated by the Controller's Office.

To illustrate these instructions, we created a sample risk assessment spreadsheet, using as an example the 2012 Public Health Service Conflict of Interest Regulations. See Attachment E.

As the complete risk assessment forms were submitted, we reviewed each and communicated with the respective Compliance Partner regarding any questions we might have and any further information the Compliance Partner reported. The next step was to create a heat map schema that

reflects the University's overall risk profile. See Attachment F. That heat map will be used to present the risk assessment process and results to the Board of Regents Audit Committee. That process follows several presentations by the Vice Presidents regarding their assessments of operational and strategic risk in their areas of responsibility.

## V. Monitoring

One final step in the process remains. We have asked each Compliance Partner to select, based on the outcome of their risk assessments, and in coordination with the responsible Vice President, a monitoring approach for each compliance area that was characterized as either medium or high risk. We view "monitoring" as a "real time" approach to testing our systems and, on a planned basis, gathering information that will reflect whether our compliance efforts and controls are effective. If the results reflect failures and/or increased risk, then the current controls or approaches likely will need to be re-evaluated. The implementation of a monitoring process enables an institution to identify problematic trends before they become wide spread. It may be appropriate in a particular risk area to systematically collect data, compare the results, and develop an appropriate action plan. The Compliance Partners, in coordination with their responsible Vice Presidents, will determine the approach. Below are examples of approaches we have offered for consideration:

| | |
|---|---|
| Inspections | Status Reports |
| Sampling | Surveys |
| Review of logs, sign-in sheets, reconciliations | Independent Reviews |
| Initialing (Documenting supervisory reviews) | Interviews |
| Spot Checks | Longitudinal Studies and Trending |
| Exception Reports | Quarterly Reports |

## VI. Frequency of Conducting Risk Assessments Going Forward

The outcomes of the risk assessments conducted will determine the timing of future risk assessments. We don't anticipate they will be conducted on an annual basis at this point. The University's Legal Compliance Reporting Process, which has been in effect since the inception of the Compliance Program, requires ongoing reporting of compliance risks and failures identified through the routine work of our Compliance Partners. The Compliance Partners responsible for compliance risk areas that are considered to represent "high" or "medium" risk are on a "semi-annual" reporting schedule. Compliance Partners responsible for "low" risk areas report annually. Should significant events occur between reporting periods, they are to be timely reported to the Compliance Office. The Director of the Office of Institutional Compliance ("Director") creates semi-annual reports of the information reported through the Legal Compliance Reporting Process for the University Auditor, General Counsel and responsible Vice Presidents. The EOCC plays a key role in addressing the compliance risks and failures identified through this reporting process. Given this infrastructure, it is anticipated that risk assessments will be conducted less frequently than what otherwise might be the case. That decision has not yet been made.

## ATTACHMENT A: 2013 LEGAL COMPLIANCE RISK ASSESSMENT

| | | | Rank H/M/L | | | | | |
|---|---|---|---|---|---|---|---|---|
| Key regulations or statutes governing your compliance areas - provide lists of key provisions or categories of provisions | Legal or policy consequences for non-compliance | Do policies Exceed, Meet, or Not Meet regulatory requirements? NA / E / M / NM | Level of Impact | Probability of occurrence | Total Level of Risk (impact + occurrence) | Is this risk owned by more than one compliance area? Y/N | Is there an opportunity to reduce burden and still be compliant? Y/N | Notes |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

# ATTACHMENT B: INSTRUCTIONS FOR THE 2013 LEGAL COMPLIANCE RISK ASSESSMENT

**Introduction**

The purpose of the 2013 Legal Compliance Risk Assessment tool is to provide an overview of the legal compliance risks within a compliance risk area (e.g. Athletics, Conflict of Interest, Environmental Health and Safety, Facilities Management, Grants Management, etc) for review by the University's senior leadership and, ultimately, the Board of Regents. The tool has been streamlined, including some yes-no questions, so Compliance Partners and others responsible for completing it should not find it too time consuming.

In reviewing the tool, the Executive Oversight Compliance Committee observed that some units are compiling similar information but in different formats. If your unit has already collected the same information that the Legal Compliance Risk Assessment requests, but it is in a different format, then you may submit that alternative document. You do not need to transfer the information into the Legal Compliance Risk Assessment tool. However, if that is not the case, please use the tool provided.

The last time a coordinated effort was made to collect risk assessments across the institution was 2002 – 2006. Although much of that data may now be out of date, it would be useful to review the results of that effort in preparation for completing the current Risk Assessment tool. Compliance Partners were sent these earlier risk assessments in November 2012. If you need another copy contact Sophia Anema.

Unlike the earlier risk assessment tool, the current version includes questions on policies and regulatory requirements as well as opportunities to reduce burden. These questions are in response to President Kaler's directive to "recalibrate our risk tolerance" in order to reduce "unnecessary administrative burden." All units need to meet their regulatory and legal obligations. The tool asks whether units are going above and beyond those obligations. More discussion about these questions is below in the instructions section.

**Timeline**

Roll out – May 14, 2013
Deadline – August 1, 2013

**Role of Office of Institutional Compliance**

Lynn Zentner and Sophia Anema are available to answer questions or consult with anyone who needs assistance in completing the Risk Assessment tool. This project is a priority for the office, especially given the tight timeline. Once all the risk assessments have been submitted Lynn will create an institutional legal risk heat map and share it with senior leadership and the Board of Regents in September.

# ATTACHMENT B: INSTRUCTIONS FOR THE 2013 LEGAL COMPLIANCE RISK ASSESSMENT

**Instructions**

"*Key regulations or statutes governing your compliance areas - provide lists of key provisions or categories of provisions*"
This column should reflect the primary regulations that drive the compliance processes you have in place in order to comply with the regulation or statute. Attached is an example that Lynn created based on the 2012 Public Health Service regulation for Conflict of Interest. Each row beneath the "PHS Reg" heading is a key provision in that regulation.

Some regulations, such as HIPAA, have numerous provisions and some have many key provisions. In this case, provisions should be grouped according to the category under which they are listed in the Code of Federal Regulations (CFR) or similar complication of final requirements.

"*List legal or policy consequences for non-compliance*"
Sometimes a regulation is very specific about the consequence for non-compliance. Last year, the maximum fine for each violation of the Clery Act (a campus security regulation) was increased to $35,000. Other times, the consequences can vary greatly, including damages from a law suit filed against the University. If consequences for non-compliance is a range then indicate the breadth of that range, for instance, "from a minor fine to possible lawsuit damages." If you do not know the consequences then list "unknown."

*"Do policies **E**xceed, **M**eet, or **N**ot **M**eet regulatory requirements? E / M / NM"*
President Kaler has requested that units examine whether our own internal policies meet or exceed the legal and regulatory requirements. In cases where the policies exceed requirements, the Compliance Partner will be asked for the rationale behind this. Sometimes there is a very good reason a policy or practice exceeds a legal requirement. The Office of Equal Opportunity and Affirmative Action uses a lower threshold of evidence when examining a claim of discrimination than would be used for a similar claim in a legal context because the University wants to foster a culture of diversity and inclusiveness. Once the deliberate decision was made to lower the threshold of evidence, the University committed the resources needed to respond to the potential increase in discrimination claims.

*"Level of Impact (H/M/L)"*
Risk assessment is not susceptible to precise measurement. The rankings will simply be a "**high**," "**medium**" and "**low**" standard. You may have specific "high risk" activities you can identify using other factors, for example, whether the activity involves human subject research, was previously listed as audit finding, or involves agreements exceeding a dollar threshold, etc. *Again, the goal is to prioritize risks within your area by considering how they relate to each other.*

The attached thresholds (Legal Compliance Reporting Standards) provide guidance as to whether an activity could produce a result that would fall into the high, medium, or low risk category.

*"Probability of Occurrence (H/M/L)"*

## ATTACHMENT B: INSTRUCTIONS FOR THE 2013 LEGAL COMPLIANCE RISK ASSESSMENT

Probability of occurrence will also be evaluated using a high / medium / low standard. In a recent presentation to the Audit Committee of the Board of Regents, Vice President Studham offered the following as a way to define these three categories. High: the probability that an event will typically occur multiple times a year. Medium: the probability that an event will typically occur one time per year. Low: the probability that an event will likely occur once every ten years. The goal for evaluating probability is to be able to determine the frequency with which an event or related events will occur.

*"Total Level of Risk (impact + occurrence)"*
Taking the rankings you assigned in the previous two columns, Level of Impact and Probability of Occurrence, what rank would you assign the risk overall? The type of impact that would occur, fines versus bodily harm for instance, should weigh in your decision of the final ranking of the risk.

*"Is this risk owned by more than one compliance area? Y/N"*
It is important for us to know which regulations apply to multiple risk areas and who, therefore, shares the responsibility of complying with them. A few common examples of shared regulations are HIPAA, FERPA, ADA, Grahm Leach Bliley Act, NCAA regulations, and the Clery Act. There may be opportunity to identify redundancies in compliance efforts as well as possible gaps. Ultimately, having a list of units that share responsibility for a given regulation will be useful to aid in the coordination of compliance efforts and avoid possible duplication.

*"Is there an opportunity to reduce burden and still be compliant? Y/N"*
As mentioned above, this question gets to the heart of the President's initiative to recalibrate risk. Is your process overly burdensome? Is it possible to ensure compliance and, at the same time, reduce the resources currently devoted to one or more of your risk areas? An example of the elimination of part of a compliance process is reflected in an e-mail the Controller's Office sent on February 12, 2013.

> **Process Change:**
> **Employee TRAVEL Reimbursement - Missing Receipts**
>
> Effective immediately the requirement to complete a separate Statement in Lieu of Receipt form (UM1566) when receipts are missing has been eliminated as it relates to the travel reimbursement process. Instead, a check box to indicate a required receipt is missing has been added to the Employee Expense Worksheet (UM1612).
>
> The revised Employee Expense Worksheet and instructions are now available in the Forms Library.
>
> We hope this paperwork reduction helps make the reimbursement process more efficient.

The simple addition of a checkbox indicating a missing receipt to the Employee Expense Worksheet eliminated the need for an additional worksheet (Statement in Lieu of Receipt) to be completed and processed. Compliance with University process and procedures was maintained but with fewer resources to do so.

# ATTACHMENT C: HIPAA/HITECH REGULATIONS

## AN EXAMPLE OF REGULATION CATEGORIES FOR USE ON THE LEGAL COMPLIANCE RISK ASSESSMENT

HIPAA Administrative Simplification Regulation Text March 2006

These regulations include the HIPAA OMNIBUS FINAL RULE released by HHS on January 17, 2013

**PART 164 — SECURITY AND PRIVACY**

Subpart E — Privacy of Individually Identifiable Health Information

§ 164.502 Uses and disclosures of protected health information: general rules

§ 164.504 Uses and disclosures: organizational requirements

§ 164.506 Uses and disclosures to carry out treatment, payment, or health care operations

§ 164.508 Uses and disclosures for which an authorization is required

§ 164.510 Uses and disclosures requiring an opportunity for the individual to agree or to object

§ 164.512 Uses and disclosures for which an authorization or opportunity to agree or object is not required 58

§ 164.514 Other requirements relating to uses & disclosures of protected health information

§ 164.520 Notice of privacy practices for protected health information

§ 164.522 Rights to request privacy protection for protected health information

§ 164.524 Access of individuals to protected health information

§ 164.526 Amendment of protected health information

§ 164.528 Accounting of disclosures of protected health information

§ 164.530 Administrative requirements

§ 164.532 Transition provisions

# ATTACHMENT D: LEGAL COMPLIANCE REPORTING STANDARDS

**Office of the General Counsel, University of Minnesota**
**Legal Compliance Reporting Standards**
**(Revised Version, 3/25/13)**

The following provides the standards for legal compliance reporting and assurance. The scope is limited to known violations of federal, state, and local law and University policy. It is recognized that University officials should receive timely reports of significant operational problems. However, operational issues are not part of the legal compliance reporting process.

Three classifications apply to compliance-related violations: (1) high, (2) medium, (3) low. These classifications pertain to the impact a violation of law or policy has on the University. Previously these classifications were "major", "significant" and "minor". The nomenclature has been changed to align with the categories on the revised risk assessment form.

Examples of general "indicators" may include:

**High:**

- Death or serious bodily injury *due to* University activity
- >$1,000,000 likely at issue
- Likely disqualification or major penalty from program (e.g. NCAA, research sponsor, etc.)
- Potential widespread and serious legal problem
- President, Chancellor, Vice President, Vice Chancellor, Dean, Head Coach, Athletic Director credibly accused of misconduct
- Requirement to report incident to an outside regulatory body with a reasonable likelihood of substantial financial or programmatic penalty
- Incidents highly likely to be accompanied by substantial negative publicity
- Circumstance is reasonable likely to result in a serious criminal charge against a University employee for University-related conduct
- Matters of significance requiring immediate escalation to the General Counsel
- Any other circumstance that meets compliance area-specific criteria for "high impact"

**Medium:**

- "Near miss" death or serious injury *due to* unsafe U activities
- Between $250,000 and $1,000,000 likely at issue
- University manager or supervisor credibly accused of misconduct
- Reasonable likelihood of a penalty from an outside body (i.e. research sponsor, NCAA, MPCA, etc.) that is not substantial and is not anticipated to interfere with University programs in the judgment of the responsible reporting party and responsible Vice President
- Potential for substantial negative publicity
- Otherwise in the judgment of responsible reporting party and Vice President is of significance to be reported to the Executive Oversight Compliance Committee as part of a periodic report
- Meets customized area-specific criteria for "medium" impact

**Low:**

- Minor safety concern or accident
- <$250,000 likely at issue
- Isolated minor legal or policy violations (violation of work rules, general HR violations, financial policies, HR policies, petty theft, etc.)

## ATTACHMENT E: PUBLIC HEALTH SERVICE CONFLICT OF INTEREST REGULATIONS

| | | | Rank H/M/L | | | | | |
|---|---|---|---|---|---|---|---|---|
| Key regulations or statutes governing your compliance areas - provide lists of key provisions or categories of provisions | Legal or policy consequences for non-compliance | Do policies Exceed, Meet, or Not Meet regulatory requirements? E / M / NM | Level of Impact | Probability of occurrence | Total Level of Risk (impact + occurrence) | Is this risk owned by more than one compliance area? Y/N | Is there an opportunity to reduce burden and still be compliant? Y/N | Notes |
| **Public Health Service 2012 regulations** | | | | | | | | |
| Scope of those subject to new regs | Federal inquiry, impact on funding | M | H | L | M | No | No | Correct scope recently re-evaluated |
| SFI reduced from $10,000 to $5,000 | Same | M | H | M | M | No | No | Need to timely capture new PHS researchers |
| Relatedness assessment | Same | M | H | L | M | No | No | |
| Frequency & timing of disclosure | Same | M | H | M | H | No | No | Beyond annually, working with grant administrators |
| Reimbursement/sponsor-ship of travel | Uncertain | M | L | H | L | No | Y - we are doing that | |
| Managing COIs | Federal inquiry, impact on funding | M | H | L | L | No | No | |
| Required reporting to PHS | Same | M | H | L | M | No | No | |
| Monitoring CMP compliance | Same | M | H | L | M | No | No | |
| Retrospective reviews and mitigation plans | Same | M | H | M | H | No | Uncertain | Working with grant administrators |
| Maintaining up to date compliant policy | Same | M | H | L | L | No | No | |
| Required training | Same | M | H | H | H | No | No | Reminder emails ignored |
| Sub-recipients - policy, disclosures, COI mgmt | Same | M | H | L | M | No | No | Few issues so far |
| Public access | Same | M | M | L | L | No | Y - we are doing that | |

**ATTACHMENT F: HEAT MAP SCHEMA**

| Likelihood | | | | |
|---|---|---|---|---|
| | High | Moderate Risk Management, low or no levels of control | Significant Risk Management, appropriate levels of control | Comprehensive Risk Management, all levels of control |
| | Medium | Moderate Risk Management, low or no levels of control | Significant Risk Management, appropriate levels of control | Comprehensive Risk Management, all levels of control |
| | Low | Accept Risk with minimal or no specific management or controls | Moderate Risk Management, low or no levels of control | Significant Risk Management, appropriate levels of control |
| | | Low | Medium | High |

**Impact**