BOARD OF TRUSTEES

Compliance, Audit, Risk Management and Legal Affairs Committee

May 28, 2015
No item in this report for release prior to (9:00) a.m. Thursday, May 28, 2015.

AGENDA

NIU Board of Trustees
COMPLIANCE, AUDIT, RISK MANAGEMENT AND LEGAL (CARL) COMMITTEE
9:00 a.m. – Thursday – May 28, 2015
Board of Trustees Room
Room 233
NIU – Hoffman Estates Campus

1. Committee Chair, Bob Boey
2. Verification of Quorum and Appropriate Notification of Public Meeting
3. Meeting Agenda Approval .................................................................................................. Action ........i
4. Review and Approval of Minutes from February 26, 2015 ............................................. Action ........ 1
5. Chair’s Comments/Announcements
6. Public Comment*
7. University Report
   a. ERM System (Enterprise Risk Management) – Al Phillips & Jerry Blakemore..................Information...9
8. Other Matters
9. Next Meeting Date
10. Adjournment
1. Consistent with Public Act 91-0715 and reasonable constraints determined by these Bylaws and the Chair, at each regular or special meeting of the Board or its committees that is open to the public, members of the public may request a brief time on the approved agenda of the meeting to address the Board on relevant matters within its jurisdiction.

2. Committees of the Board review University proposals for action and make adjustments and endorsements as appropriate for further consideration by the full Board. Public comments are generally most useful at meetings of Board committees, where proposals are first considered and the time for interaction most feasible.

3. To facilitate an orderly process, appearance requests must be registered on a Board-provided form and submitted to the Board’s Parliamentarian at least 45 minutes before the meeting is scheduled to be called to order. To be recognized, the appearance request will include the name, address and position of the individual wishing to speak, the name of the organization or group represented, a concise summary of the presentation, and whether the requestor has appeared earlier on the topic before any other meeting of the Board. The Parliamentarian may confer with registered speakers to cooperatively assist the Chair of the meeting in assuring coordinated issue presentation and an efficient use of allocated time. The Parliamentarian will acquaint requestors with the generally acceptable rules of decorum for their presentations. In lieu of oral presentations, individuals may present brief written materials not to exceed five (5) pages to the Parliamentarian for distribution and consideration by the Board in advance of the meeting.

4. The Chair of the meeting will recognize duly registered individuals at the appropriate point during the meeting. Unduly repetitive comments may be discouraged and restricted by the Chair. To assure an orderly and timely meeting the Chair may limit time allotments to five minutes or less, may delay or defer appearances when appropriate, and defer or refer questions received from presenters for answers if available.

Anyone needing special accommodations to participate in the NIU Board of Trustees meetings should contact Ellen Andersen, Director of Special Events, at (815)753-1999, as soon as possible, normally at least a week before the scheduled Board meeting.
CALL TO ORDER AND ROLL CALL

Time: 10:25 AM

Present: Trustees Wheeler Coleman (WC), Robert Marshall (RM), Cherilyn Murer (CM), Marc Strauss (MS), Student Trustee Paul Julion (PJ), Board Chair John Butler (JB), Committee Chair Robert Boey (RB)

Phone: N/A

Absent: Trustee Anthony Iosco (AI)

Extras Present: President Douglas Baker, Committee, Board Liaison Mike Mann, Provost Lisa Freeman, and Board General Counsel Gregory Brady

Asked for roll call: RB: I'll call the meeting to order. Good morning and welcome to the meeting of the Compliance, Audit, Risk Management and Legal Affairs Committee fondly referred to as CARL Committee. The only person who uses that word fondly referred to is Jerry Blakemore. I will now call the CARL Committee or order and ask the administrative secretary Julie to take the roll call please. Miss Edwards.

Performed roll call: JE

VERIFICATION OF APPROPRIATE NOTICE OF PUBLIC MEETING

Chair: JB: Mr. Blakemore do we have quorum and appropriate notices under the Illinois Open Meetings act?

Answered verification: Board General Counsel JB: We do Mr. Chairman.

MEETING AGENDA APPROVAL

Chair: RB: May I have a motion to approve the proposed agenda?

Motion: CM: So moved.

Second: MS: Second.

Chair: RB: All in favor?

All: Aye

Chair: RB: Opposed? Carried, thank you.

REVIEW AND APPROVAL OF MINUTES

Chair: RB: May I have a motion to approve the minutes of November 6, 2014 on the CARL Committee minutes?

Motion: MS: So moved.
Second: PJ
Chair:  RB: Discussion? All in favor?
ALL: Aye.
Chair:  RB: Opposed? Carried, thank you.

PUBLIC COMMENT

Chair: RB: Mr. Blakemore any requests?
Legal: JBI: We’ve had no requests for opportunity for public comment Mr. Chair.
Chair: RB: Thank you.

CHAIR’S COMMENTS/ANNOUNCEMENTS

Chair: RB: Let me take a moment off of my remarks as CARL Committee chair, let me begin by thanking each of you for attending this meeting and I would like now to recognize the various leader of the university constituent groups. Dr. Bill Pitney. Deborah Haliczer, President of SPS Council and Dr. Gregory Waas. Good morning. Thank you all three for coming this morning and Jay Monteiro President of Operation Staff, Jay good morning. Thank you. We’re especially pleased that you’re with us today. Any remarks that you would like to share with us today, all four of you, any remarks? None. Thank you. The agenda for the CARL committee involves update on three important areas of our jurisdiction and these areas include property insurance validation; the gubernatorial changes; governmental changes and ethics; enterprise and risk management. Given that the board has extensive committee agenda and will also be meeting in special session, I want to limit our total discussion of the university reports to approximately 30 to 40 minutes. So let us proceed. Property and insurance validation by Sara Cliffe, Director of Compliance Administration. Sara.

Sara Cliffe: Good morning.

JB: Good morning.

Sara Cliffe: I’m here to talk about the total insured values that we submitted as part of our property renewal two weeks ago. And what I’ve provided is a chart that compares our total insured values which includes everything, our buildings, our contents and our artwork, compared to the values that we submitted last year and I’m going to talk briefly about the increase or decrease. Buildings decrease due to the demolishment of Douglas Hall otherwise there was a 2.3 percent increase as recommended by MEC and per one of the carriers, the 2.3 represented the lowest inflation rate among the states of members who participate in the MEC program. I also examined the engineering news reports building cost index for a comparison and for the year building costs increased by 2.9 percent. So what happens is generally for our buildings they are automatically increased by the 2.3 percent unless we have some other valuation to go by. We did receive information on Northern View and New Hall provided by the owner but that’s what happened with buildings. With contents, they generally increase due to the one percent increase recommended by MEC as well as departmental input from those whose content values fluctuate such as ITS, Doc. Services, Holmes Student Center, the Material Distribution Center, etc. We send out inquiries as it relates to their inventory and their contents and they send it back into us and so there was an increase in contents. Fine arts, including special collections, which means the art on campus as well as the library’s rare books and special collections at Founders increased and we have artwork all over campus, but for Latino Center, Rockford Education Center, and then the School of Art particularly. The library collection which does not include the rare books and special collections increased per the
values reported by the library and Dean Dawson. Now builders risk we did not report any builders risk for last year which is the insurance for if something happens during the building or the demolition of the building, but we did this year for Stevens building, the Grant roof and the Lucinda Avenue extension project. So we reported the value of close to 25 million. And then business interruption which is revenue that the university would lose should we have to shut down operations for a period of time increased. We had a new form this year that actually took into consideration deductions not previously contemplated, so it didn't increase as much as it may have otherwise but it did increase. And so overall we have a 1.54 percent increase. Last year's I believe was a 6 percent increase which will be good news when it comes to premium time because your total insured values is one of the major driving factors. So that's the general idea of what we submitted and what our insured values are.

RB: Great. Thank you. Yes go ahead Cherilyn.

CM: What is our policy on appraisals and reappraisals of the art collection and the rare books?

Sara Cliffe: We get that information from the library, I don't know if they did it this year, but last year they did compare.

CM: But do we have an outside appraiser come in and look at giving us an appraisal on the art and on the rare books that then is used as the basis of this element of the policy?

Sara Cliffe: I don't believe so.

CM: Is that something to think about at least?

Sara Cliffe: Yeah it would be a good idea.

CM: Because usually that art and rare books sometimes needs a different type of insurance. I'm interested in this and it would be interesting also to determine what the appraised value is on our art, especially the Southeast Asian collection which we need to really be protective of. If you could get back to the committee or to the chair, I have an interest in that.

Sara Cliffe: Sure will. I can tell you we also have other insurance policies that are purchased for specific collections of art like the School of Art and the Anthropology Museum and they have their own so this is our property that kind of sits above those, and they may do appraisals as part of those smaller policies. I'll find out and provide the information.

CM: But I'm interested in this also especially since this is a major area for the university. Our collections are of great value as an asset so if you could give me more information I'd appreciate it.

Sara Cliffe: I'd be happy to.

CM: Thank you.

RB: Trustees any other questions? No, okay. Thank you Sara for an excellent report and we appreciate the work that you and your staff do. Mr. Jim G, where are you Jim.

Jim Guagliardo: Good morning members of the board. This is going to be a pretty brief presentation. Basically Governor Rauner has issued some executive orders which have added to the ethics requirements of the State Officials and Employees Ethics Act. One has to do with the revolving door prohibitions. These are the WHEREAS, these would be the rationale for doing so. I'm not going to read them but the basic rationale the governor is that we can always have a higher code of ethics and he decided to change some of these laws, or attempt to change some of these laws through executive orders. That's very controversial and I'll talk about that in a moment. One of the changes on the next slide is the Revolving Door Ban. Just basically makes it more difficult for employees, state employees, to
go from state employment to lobbying employment. While you’re a state employee you’re not to negotiate with a lobbying firm or try to set a salary with a lobbying firm. That’s a new requirement under these executive orders. Also no former state employee within a year after leaving his or her position with the state agency shall accept any compensation from a person or an entity for lobbying. So there’s a waiting period that was added for people who leave state employment and go into lobbying. These, just to be clear, were already lobbying restrictions in the state official’s employee’s ethics act in the Illinois procurement code and these were added to those restrictions, they are not in lieu of the restrictions. One thing that probably is going to affect the average NIU employee more than the lobbying provisions is the gift and travel ban. There used to be a $100 cap on gifts. We obviously as a university do a lot of business with a lot of different vendors and every once in a while a vendor will gift an employee something; a Kindle. I’ve had that circumstance come up a couple times where a vendor will give an employee a Kindle. Unfortunately those are worth more than $100 so you can’t accept that, but they’ll often give gift certificates for $75.00, $80.00 and I get the question as Ethics Officer well can I keep this? And there was a pretty black line rule that if it’s under $100 yes you can keep it; if it’s over $100 no you can’t keep it. If it’s $101 no, if it’s $100 yes. The Governor has issued this executive order just saying no, no gifts at all from anyone for any amount, not even a stick of gum. The issue is, and I asked the Executive Director of the Executive Ethics Commission does this apply to us here at Northern Illinois University? Do these executive orders apply to us? And he said it’s up to you. I said okay I’m glad I called. I said I hope you don’t mean me, me, I hope you mean NIU. And he said yeah NIU, it’s up to NIU. I don’t think the governor has the power to do this by executive order for universities. This is him speaking, I think it’s an over reach of power. I said okay keep talking, keep telling me this. Executive orders under the constitution are basically for things like reorganizations. They’re not to substantively change laws and indeed these seem to be substantive changes to the State Officials Employees Ethics Act. Clearly, this goes beyond reorganization. Clearly this goes beyond what executive orders can do. However, an agency can always add to the ethics laws of the state. In other words, your ethics restrictions can be more restrictive than the state law if you want. So arguably the governor’s executive orders do have affect, certainly in the governor’s office they do, and a better argument can be made for agencies that are more closely associated with the Governor’s office. When you get to the university level, then you’re getting a little tenuous. What the Executive Ethics Commission has done has asked the Attorney General for some guidance here. What agencies are really bound by these executive orders and they’re still waiting to hear from the Attorney General. If they don’t get a formal written opinion, those sometimes can take a long time, they’re looking for some guidance. In the meantime, the Executive Ethics Commissioner said for the ethics commission itself, they’re going to follow these standards and he literally said it’s up to our agency whether we follow them or not. I learned this very recently and I have not had time to talk to the institution on this so I just lay it out there for discussion or for any consideration if we want to discuss it at a different time or publically.

RB: We have a question by Trustee Coleman.

WC: I don’t know, Jerry or Dr. Baker if you don’t mind answering this question, what’s your position on this?

JBL: The Office of General Counsel and the general counsels for all of the public universities have looked at the issue of the extent of the authority of the governor to use executive orders to promulgate new rules and regulations. What the Ethics Officer has said is correct in the sense that executive orders actually implement authority that’s already been authorized by a statute and if you go beyond that statute then the executive order does not have any real legal meaning or not. However, there is a consensus amongst particularly the president and other presidents and chancellors that universities should take every opportunity to comply with the spirit of the executive order and this is one of those examples where the spirit of the executive order says that we should not be taking gifts that in any shape, form, or fashion that may influence the decision that is made or add factors that are not relevant to that decision. So to the extent that it is practical, we will comply with the spirit would be the advice here. There are certain situations where if you are at an event and they’re serving food, you don’t want people thinking they can’t eat the food that’s available to everybody because it could be perceived as a gift. Well it’s not and part of what my office and the ethics officer will do is take those particular fact
situations and provide an opinion. But the overall point is we should comply with the spirit. The ethical requirements are by their very nature, they go beyond what the legal requirement is. That is how we will look at this.

CM: What comes to mind Jerry when you speak of this when you talk about food, it just brings to mind renowned Supreme Court justice who said you know it when you see it. And I think we need to live by that. There should be an instinctiveness that you know it when you see it and it's not about roast beef sandwich or even gift certificates. Gift certificates to me, regardless of what the value is, whether it's $80, that to me rings a bell differently than does it meet the letter of the law, yes but why is somebody giving anybody a gift certificate is the question and I think that should be the spirit of how we address ethics within our university.

Douglas Baker: I think Jerry is right on target with his comments on abiding by the spirit of it. Sometimes the spirit is a little fuzzy though on what's prohibited. So let's say we're forming a relationship with another university and the president comes to my office and presents me with a framed photograph of his campus, gifting me a photograph of his campus. Okay.

CM: The value is just what the frame is and so if it were a 24 caret gold frame, I'd probably have a question. If it's a frame that you get at wherever then it's worth $20.00.

Douglas Baker: But if it's zero I can't take it, I've got to give it back to him. We've got to kind of figure out some of that stuff.

RB: And the photograph shows his office.

Douglas Baker: Right that's what I meant, a picture of the school, should we accept it to memorialize our relationship with them or is that something else. Maybe I'm getting too much into the nuance, we need to subscribe to the spirit of this and figure out how to apply it and then wait for the Attorney General to give everybody an opinion.

WC: I kind of agree with Jerry that we should abide by the spirit of this executive order that was issued. I think then the next question would be then what policy changes do we need to do as an institution to kind of follow the spirit here?

JBL: I think there are two things that have to happen and when Jim and I had this discussion earlier, this was prior to actually having an opinion from the Executive Director which he actually received today. One, I think we are going to have to establish a policy for this and indicate even more important that the policy which would be complying with the spirit, that we will have a mechanism to make those determinations. Right now those type of opinions go to the Ethics Officer and that decision would be binding, in my opinion, and we need to make that clear as part of our procedure, but we also need to make sure that we have the resources to sort of do that because you can really get inundated with these types of requests. I would suggest that such a procedure establish a database so that we are consistent there, but this is a particular issue especially as we look to do more in the international affairs arena. Where we want to give gifts as we are traveling, we want others to provide documentation or memorialize who they are for us. The whole discussion we just had about art, that's a big part of, so we cannot ban gifts, but we really do need to provide some parameters and part of that parameter would be materially relevant to the institution and not the individual. So that would be one of the criteria.

WC: So that would be the distinction here right, so if Dr. Baker received a framed picture of another institution, is it his personally or is it a gift to the institution and can we accept that on behalf of the institution versus individually?

JBL: Correct. It would be on behalf of the institution and again, the institution is not banned from receiving gifts in the course of its mission, but the individual would be banned from receiving gifts.
WC: And that’s a big difference.

JBL: Right.

RB: And I think that Trustee Coleman said, as we get more and more involved in the international arena, those gifts subjects really come into play, if you turn down somebodies gift, in many cases it’s a slap in the face. You have to be careful in that respect too. So it’s a touchy business.

WC: So I need clarification here, today we cannot, for federal employees; we cannot provide them with gifts. Is that correct?

JBL: There is a federal ban; they have the same types of ethics requirements. I’ve not reviewed them in detail, so generally I would say that is correct to the extent or where there are exceptions, that I’m not certain of.

WC: Okay. So what I’m trying to point out to you, I don’t think – this executive order I believe it’s in keeping for the federal employees as well. So this is very similar to what’s in place for the federal employees and it doesn’t have a dollar limit on gifts, it’s saying absolutely no gifts. So this is not totally out of line. I think as an institution we probably should step back and say how do we abide by the spirit of the law or the executive order.

CM: What is the travel portion of the ban?

Jim Guagliardo: I’m sorry?

CM: The travel portion of the ban?

Jim Guagliardo: Well the travel portion is, again the gift ban applies to prohibitive sources, it doesn’t apply to the university paying for people’s travel to do their jobs, it’s for instance, if Microsoft is going to hold a conference and Microsoft wants to pay your travel, there’s a procedure, there really isn’t a ban amount. For travel, the rule is is it really work related. In other words, is Microsoft having you come to a conference where you’re going to learn things that are going to help you do your job, if so, they can pay for that and there’s no limit to that. If they’re going to send you to, I don’t know, Boca Raton for a weekend on the beach which has nothing to do with you learning your job, no. One of the changes in the executive order was it used to be the institutions Ethics Officer that would review that and determine whether or not it was education related or mission related for employees, it’s now the Executive Ethics Commission that makes that determination under the new executive order. The executive orders are a little bit more complex than what the PowerPoint shows so the rule is not so much an amount, is it admission related, is it educational related, does it help you do your job? If it does, a prohibited source like Microsoft or any vendor can pay for it. If it isn’t, they can’t.

RB: Chair Butler?

JB: I would first like to say that we have an Ad Hoc Committee on Governance and we are working on a number of policies. We might take this up in that context and consider how we might incorporate some of these expanded ethics requirements in that. I’m a little bit more interested in the revolving door provisions can you tell me what’s different about the new provisions, the executive order provisions, and the current law?

Jim Guagliardo: I can tell you that the lobbying ones have gotten stricter. Exactly how they’ve gotten stricter I can’t tell you off the top of my head, I don’t know if Jerry can or not. I don’t know if the one year waiting period is obviously shortened from what it was, I’m not sure what the waiting period was before, and I assume that there was not an all-out prohibition of a state employee talking to a lobbying organization before, whereas now you can’t even start to negotiate with a lobbying organization or a registered lobbyist organization if you work for the state.
JBL: The only thing that I would add to that and I think Jim is right on point is that under the new provisions there used to be a manner in which you can get an exception from the commission for the lobbying issues, that possibility has been eliminated. So there is no process of going to the executive commission now to say given the unique circumstances I should be exempted from this rule. So they've eliminated that as a possibility.

JB: So the board understands this, by state employee it also means board member?

Jim Guagliardo: Yes.

JB: So if we were to be no longer serving on the board, if our terms expire for whatever reason, we would be subject to these revolving door provisions?

Jim Guagliardo: Yes.

JB: So I would ask us to be very cautious about that in that regard because I don't think we necessarily want to invite higher burdens if they don't make sense for us if they are disconnected from our duties as trustees, if they don't involve any entities for example that relate at all to Northern. We don't want to add that extra burden on to ourselves and absorb that extra professional limitation that we don't need to absorb because it involves entities that never did business with NIU and proposals that never came before us as board members.

CM: I have a question on that, on the revolving door. My understanding though is that's not applicable to the legislature, the state legislature?

Jim Guagliardo: I don't know.

CM: Is that correct that it is not? So it's applicable, so let me put this in perspective, it would be applicable to a trustee as John has just spoken of, but apparently it is not applicable to the state legislature?

JBL: The state legislature and the other constitutional officers have their own ethics requirements which are different.

CM: And the revolving door is not part of it.

JBL: And the revolving door is not part of it, surprise, surprise. That is correct.

RB: Any other questions? We'll now move on. Thank you Jim for an important update. We'll now move to Enterprise Risk Management presentation, Miss Danza.

Michele Danza: On February 10th we posted an RFP, a request for proposal, for enterprise risk management and the responses are required, actually we pushed that out a little bit because we did have some questions from some of the bidders which were responded to today and so the new date for responses is March 4th is for the responses to be required. The requirement is for a consulting firm who is experienced in an organization of our size and scope and mission. Who is familiar with the risks involved and who can guide us and this is for facilitation and guidance, who can guide us in assessing what we already have in place in certain pockets around the university and tying those together and seeing where there are gaps and in making recommendations on how we can infiltrate this throughout the culture as well as documenting them and reinforcing them in the policies and procedures that we'll have in the future. So it's intended to take disparate pieces and combine them so that we can have a comprehensive enterprise risk management philosophy and system.

RB: Great, thank you. Questions trustees? Trustee Marshall?
RM: Will there be, in the future, follow up on proposals to tweak the activity?
Michele Danza: Yes if that is found to be a need that we need to in a sense hire out for that expertise then yes, I’m assuming that we would have those proposals?

RB: Any other questions? Well thank you Miss Danza for a very nice presentation. Thank you.

<table>
<thead>
<tr>
<th>UNIVERSITY RECOMMENDATIONS/REPORTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Item 7.a – Property Insurance Valuation – Sara Cliffe</td>
</tr>
<tr>
<td>Information Item 7.b – Gubernatorial Changes in Ethic Requirements – Jim Guagliardo</td>
</tr>
<tr>
<td>Information Item 7.c. – Enterprise Risk Management Initiative – Michele Danza</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>OTHER MATTERS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chair: RB</td>
</tr>
<tr>
<td>Speaker: N/A</td>
</tr>
<tr>
<td>Chair: Robert RB</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>NEXT MEETING DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chair: RB: The next meeting of the CARL Committee is scheduled for May 28, 2015. Thank you.</td>
</tr>
<tr>
<td>Actual date/time: Tentatively, May 28, 2015</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ADJOURNMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chair: RB: With that I’ll now close the meeting unless there is some other discussion. May I have a motion to adjourn?</td>
</tr>
<tr>
<td>Motion: CM: So moved.</td>
</tr>
<tr>
<td>Second: MS</td>
</tr>
<tr>
<td>Chair: RB: All in favor?</td>
</tr>
<tr>
<td>ALL: Aye.</td>
</tr>
<tr>
<td>Chair: RB: Opposed? Carried, thank you.</td>
</tr>
<tr>
<td>Meeting adjourned at: 11?</td>
</tr>
<tr>
<td>Respectfully submitted,</td>
</tr>
</tbody>
</table>

Julie Edwards  
Recording Secretary

In compliance with Illinois Open Meetings Act 5 ILCS 120/1, et seq, a verbatim record of all Northern Illinois University Board of Trustees meetings is maintained by the Board Recording Secretary and is available for review upon request. The minutes contained herein represent a true and accurate summary of the Board proceedings.
I. WHAT IS- AND ISN’T- ENTERPRISE RISK MANAGEMENT

A. The Case for ERM- "Why it's worth it"

- Why we need a broader approach
- What's driving implementation
- What is it, exactly? Definitions and standards:
  - Consultants' Definitions
- Key business benefits

B. The New Landscape of Risk Management

- Failures, barriers and challenges
- Contributions from AGB, EAB and APQC
- Keys to success

C. Defining Enterprise Risk Management

Enterprise Risk Management (ERM) is a broad-based approach to managing risks on campus. It is a term of art that is helpful as a way to differentiate the practice from more traditional, insurance-based approaches to managing risk. There are multiple definitions of ERM; our session will review the key standards in use. Two key sources are the International Organization for Standardization (ISO) and the Committee of Sponsoring Organizations (COSO)
In 2009, ISO published a standard on the practice of risk management that defined risk management as "a coordinated effort to direct and control all activities related to risk." It defines "risk" as the "effect of uncertainty on objectives," thereby linking the management of risk to what is most important to the organization. Another key foundation of the practice is that the responsibility for managing risk is spread across the organization to those who have accountability and authority to manage those risks - risk owners. The ISO 31000 Standard on the Practice of Risk Management has been widely accepted in countries around the world, while implementation in the U.S. has lagged. With the impending publication of ISO 31004 (expected in September of 2013), the Implementation Guide, there will likely be even more support for this international standard. All ISO standards are reviewed and updated on a five-year cycle, so it is assured that the practices and guidance remain current.

Published in 2004, the COSO ERM Framework describes it as "a process, effected by an entity's board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives." (Committee of Sponsoring Organizations of the Treadway Commission, 2009).

The COSO ERM Framework has been embraced by organizations that are held accountable to the provisions of Sarbanes-Oxley, financial institutions and organizations with strong internal audit functions. It is widely regarded as difficult to implement in organizations that lack a top-down mandate or clear hierarchy of accountability.

D. What ERM "Isn't"

ERM is not:

- "Something we're already doing; we just don't call it that.”
  If your institution manages some risks in "silos" (with separate leadership, little or no communication and no cross functionality), then you're not implementing ERM. It is very intentional and transparent.
- Just an integration of all risk management functions.
  If you do not link risk management to strategy, mission and objectives, then you are not practicing ERM. If you do not apply the process to decision making, then you are not practicing ERM.
- A way to eliminate risk.
  Risk is not always bad; we must embrace risk in order to pursue an objective or a new path. ERM allows an institution to take risks wisely, understanding the potential impact of uncertainty upon its goals and objectives.
- A quick fix.
  It typically takes 3-5 years to fully implement. Building understanding and support and changing culture takes time!
II. Legal Counsel's Role in Enterprise Risk Management

A. The Lawyer's Duty

From the early lessons in law school, it was drilled into the minds of law students that they must exercise diligence and zeal in advocacy for their client. Rule 1.3 of the ABA Model Rules of Professional Conduct states "A lawyer shall act with reasonable diligence and promptness in representing a client."

The ABA Model Rules go on further to define a lawyer's obligations as a counselor and advisor in Rule 2.1:

In representing a client, a lawyer shall exercise independent professional judgment and render candid advice. In rendering advice, a lawyer may refer not only to law but to other considerations such as moral, economic, social and political factors, that may be relevant to the client's situation.

While not specifically enumerated as an "other consideration" in Rule 2.1, giving advice to a client about risk and its implications and options for managing risk could easily fit within the obligation of a lawyer as counselor or advisor to her or his client. Whether in a reactive or proactive sense, lawyers practice risk identification, assessment, and management on a daily basis on behalf of their client.

Finally, legal counsel to a college and university has an ethical responsibility to the entity. ABA Model Rule 1.13(a) states: "A lawyer employed or retained by an organization represents the organization acting through its duly authorized constituents.” Thus, can it be said that legal counsel has an ethical and professional duty to the Enterprise to exercise diligence and zeal in rendering judgment and advice on such matter as Risk Management relevant to the college's or university's situation? Stated differently, what is the role of legal counsel in Enterprise Risk Management?

B. Standard & Poor's View of Enterprise Risk Management

As noted above, there are a number of models or frameworks for Enterprise Risk Management such as COSO or ISO. One consultant has defined Enterprise Risk Management as: "A rigorous approach to assessing and addressing the risks from all sources that threaten the achievement of an organization's strategic objectives.” Micclos and Shah, Enterprise Risk Management, An Analytic Approach, (Tillinghast-Towers Perrin, 2000).

Enterprise Risk Management has caught the attention of financial ratings companies such as Standard & Poor's Ratings Services. According to Standard & Poor's Rating Services, "This enterprise risk management initiative is an effort to provide more in-depth analysis and incisive commentary on the many critical dimensions of risk that determine overall creditworthiness." http://www.standardandpoors.com/ratings/emr/en/us Rather than focus on a particular definition of Enterprise Risk Management or a specific approach or framework, Standard and Poor's leaves that up to the organization. Standard & Poor's focuses on the institution's culture

The National Association of College and University Attorneys
(communication, frameworks, roles, policies, metrics and influence) for managing risks and its strategic risk management (identification and updating process and impact on key decisions). See, Standard & Poor's To Apply Enterprise Risk Analysis to Corporate Ratings, May 7, 2008.

C. Can you "C" Enterprise Risk Management?

As legal counsel for a college or university determines her or his role in Enterprise Risk Management, one must understand the letter "C," according to the Association of Corporate Counsel? www.acc.com

1. CLO - Chief Legal Officer: This term is increasingly being used to describe the in-house, head of the law department in a private corporate setting.

2. CRO - Chief Risk Officer: With the emergence of Enterprise Risk Management, this term is being used to describe the head of the risk management function at an organization.

3. CCO - Chief Compliance Officer: With the adoption of the Sarbanes-Oxley Act of 2002 (SOX), publicly-traded companies are required to improve corporate transparency and accountability. In response to SOX and subsequent regulations, a number of organizations established a centralized compliance function for overseeing and/or reporting on the institution’s compliance.

D. From Traditional Risk Management to Enterprise Risk Management

Traditional risk management began more as a transactional function of a college or university focused around the purchase of insurance with claims being handled by the insurance company. Said differently, the focus of risk by the institution was to transfer it by purchasing insurance. Insurance was typically handled by the business office of a college or university and often purchased through a process of Requests for Proposals. The CLO focused more on the insurance contract. When claims arose, the insurance company coordinated the legal defense of claims.

As risk became recognized as an expense to the college or university, risk management became more integrated within the business operations of the institution with an increased emphasis on proactively looking at certain risks and the exploration of options of risk transfer such as risk-sharing pools, captive insurance companies, and self-funding of claims. The role of the CLO increased in the involvement of this transactional approach to risk management. The emphasis was still weighted more towards reactive (claims and litigation) than proactive risk management.

Today, Enterprise Risk Management is gaining momentum as a systemic approach to evaluating risks and aligning the risks and management of them with the entity's strategic goals. Increasingly, top administration and governing boards are becoming engaged in Enterprise Risk Management and the CRO is becoming more prevalent its facilitation. Further, the CLO becomes more proactive in assisting the institution in overall risk assessment, prioritization, and alignment with strategic goals and is a stronger collaborator with risk management function.
E. Legal Counsel and Engagement in the Enterprise Risk Management Process

As an institution considers advancing to an Enterprise Risk Management model, if an outside consultant is to be used to assist, legal counsel might consider retaining the consultant and have the consultant work through the advice and direction of counsel in an attempt to protect such work from subsequent discovery, which may only be effective in certain jurisdictions.

Depending on the model or approach used by an institution, an Enterprise Risk Management process could involve seven steps or phases. There are key steps or phases where legal counsel should, in particular, look to engage. As the institution enters the risk identification step or phase, this involves an assessment of real and perceived risks. It is important for legal counsel become involved early to understand the process and the documents likely to be created as it is possible that such documents could surface during the discovery process of subsequent litigation.

Another important step or phase involves an analysis of the risk treatment options. Legal counsel can be helpful in providing advice and counsel as the various options are explored. When the Enterprise Risk Management involves the implementation of risk mitigation step or phase, legal counsel can assist the institution in the development of policies, procedures, and protocols to effectively manage the identified risks. As Enterprise Risk Management is an on-going and sustainable process, legal counsel should be involved in providing counsel and assistance to institutional representatives regarding monitoring and adaption in the management of the enterprise's risks.

F. To Whom the CRO Reports

With the appearance of Enterprise Risk Management and CRO’s and increasing government regulation and compliance functions and CCO’s, institutions are re-examining how they structure themselves to address these areas. Further, the tightness of institutional budgets is also driving a consolidation of functions. According to a NACUA Survey conducted in 2012, over 500 Chief Legal Officers of member institutions were surveyed and “Seventy-five percent of the respondents mentioned compliance and government regulation as a trend in the practice of higher education law.” In that same survey, a number of concerns were noted about the changing and expanding role of general counsel at a college or university, including:

Multiple, sometimes conflicting responsibilities ("Board secretary, compliance officer, policy guru, government relations, labor relations ...In these days of more complexity and tight budgets, it is likely I will wear more hats, not fewer.")

Perceived role as "compliance officer" ("the challenge of maintaining the sense of the GC as a counselor and advisor to all Board level and administrative constituencies, and not a 'compliance' officer.")

For colleges and universities, compliance is an enterprise risk although it is rare to find a CCO reporting to a CRO.
1. CRO reports to CEO- Standard and Poor's notes that only a few companies they have rated a CRO with enterprise-wide responsibility reporting to the CEO, but their numbers have increased in recent years, particularly in the energy sector. Some firms are developing the role, although most companies have, at this point, decided that other executives can carry out the functions of a CRO. *Credit FAQ: Standard and Poor's Looks Further Into How Nonfinancial Companies Manage Risk.* June 24, 2010.

2. CRO reports to CFO- At The Ohio State University, Enterprise Risk Management provides a formal and continuous process to identify, assess, prioritize and manage risk exposures and opportunities across the institution. It is designed to identify potential events that may affect the university, to manage risks within its risk appetite and to provide reasonable assurance regarding the achievement of the university's objectives.
   http://busfin.osu.edu/riskmgmt/default.aspx

3. CRO reports to CLO- At Yale University, the Office of Enterprise Risk is a suboffice of the Division of the Vice President and General Counsel. It directs a comprehensive enterprise risk program. ERM is a resource for University managers and other members of the Yale community to obtain management (ERM) coordinates the University's risk management efforts risk management advice so that they can carry out University activities in a manner that adequately considers safety, financial, reputational, and other risks. ERM also has primary responsibility for negotiating and ensuring the sufficiency of the University's insurance portfolio and other risks and loss control programs.
   http://ogc.yale.edu/riskmanagement

At Grand Valley State University, the Office of Risk Management is a part of the University Counsel Office in the President's division. Centralized University services provided by the department include:

- Coordination of the University's Enterprise Risk Management
- Questions or issues related to the University's property and liability insurance programs
- Insurance negotiations and purchase
- Contract review for insurance requirements
- Certificates of Insurance
- Claims administration
- Risk management consultations
- Loss control and loss prevention assessments
- Facilities and site surveys
- Questions related to practicum or internship agreements http://www.gvsu.edu/uco/riskmanagement/

See, also, the excellent outline from the 2012 NACUA Annual Conference titled *Hat Trick: Can a Chief Legal Officer Manage Nonlegal Functions*, Elise Traynum (Moderator), University of California Hastings College of Law, Tom Dorer, University of Hartford, Paul J. Ward, Southern Methodist University, and Ellen M. Babbitt, Franczek Radelet P.C.
G. Ethical considerations- Attorney/Client Privilege & Attorney Work-Product

As noted above, a part of an Enterprise Risk Management process involves risk assessment through the collection and categorization of data for analysis is an important part of the process. As various campus constituencies are sought out for their impression of the likelihood of a risk, its potential financial impact, and their evaluation of the management controls, this information is important for college or university administrators making future decisions about risk and its effective management. Also, such information can be a treasure trove for a clever plaintiff's counsel looking to prove the institution was aware of the risk and failed to adequate precautions. As institutions are engaging in risk analysis and enterprise risk management, it is important for legal counsel to review the attorney-client privilege and its application and, especially its limitations, to enterprise risk management.

In Upjohn Co. v. United States, 449 U.S. 383 (1981), the U.S. Supreme Court acknowledged that the attorney-client privilege is the oldest privilege for confidential communication known to common law. Federal Rule of Evidence 502 codifies the attorney-client privilege to protect confidential attorney-client communications. In many jurisdictions, state law differs from federal law. As institutional counsel is sought for advice regarding risk assessment and data collection in enterprise risk management, a review of extension of the attorney-client privilege and its limitations is important.

As for attorney work-product, federal law and state law may vary as to whether documents and tangible things otherwise discoverable can be protected from discovery when they are not prepared in anticipation of litigation or trial. Therefore, legal counsel should be wary relying on the attorney work-product doctrine for protecting documents created through an Enterprise Risk Management process.

There are a number of excellent and rather extensive outlines that have prepared and presented at prior NACUA conferences and the following is a listing of some of those outlines to which you might refer:

Current Trends Involving Attorney-Client Privilege and the Higher Education Attorney, Phyleccia Reed Cole, Senior Associate General Counsel, Southern Illinois University Edwardsville, June 27-30,2012

Attorney-Client Privilege on Campus, Christopher C. Marquart, Alston & Bird LLP, Atlanta, Georgia, June 27- 30, 2010

Role of Inside/Outside Counsel- Who is the Client and What is Privileged? Robert Clayton, Shareholder, Littler Mendelson, P.C., Aylson J. Guyan, Associate, Littler Mendelson, P.C., Dana Scaduto, General Counsel, Dickinson College, March 5-7, 2008


III. Tips for Implementing/Operating Enterprise Risk Management on a Shoestring
After the context is established and the risks identified, analyzed and evaluated, the work begins on how best to treat these risks. It must be admitted that the first parts of the process can be very interesting, and even exciting, and bringing together various departments and stakeholders into the process can feel quite satisfying. But now comes the part where those departments who had a little bit of fun identifying and quantifying the risks, now must be called upon to report their work to date and come up with a plan for formalizing the future treatment of any risks assigned.

Below are some tips for implementing a formal ERM process with very little cost and without adding an enormous workload to the General Counsel, CFO, risk manager, or internal auditor. One of the greatest impediments to getting things started is the perceived enormity of the process, but these suggestions can help the ERM champions within the organization to understand that the vast majority of the work will be performed by others and that their role is predominantly oversight and cheerleading.

1. Assignment of Risk Owners-
The only way for senior administrators to adequately manage the process is to push accountability down the organization to people with the abilities and subject matter expertise to oversee the treatment of a risk. That “risk owner” may further delegate certain tasks to others, but they must remain ultimately accountable and responsible to report their activities back to senior management. Establishing an ERM committee is highly advisable, but senior management must be prepared to keep the process moving.

2. Need for a System-
This process of risk owner assignment and reporting takes a system. Even some very sophisticated institutions will use spreadsheets, but there are reasonably-priced, web-based platforms available that allow for the cataloging, delegation and reporting of risks. Senior administrators would then have access to check on progress and produce reports suitable for the board level.

3. Best Practice Resources-
In today’s connected world, and given the continued collegiality among higher education institutions, best practice examples among our peers abound and are often easy to find with a simple web search. The University Risk Management and Insurance Association (URMIA), also has a library of best practices for their members as well as the ability to post questions to their community discussion forum. For those members of United Educators, they also provide an extensive library of well-researched white papers.

4. Reporting of Activities and Success-
Any ERM program must include reporting up through the institution and eventually to the board level. Risk owners should regularly be letting senior management know their agendas and their progress toward agreed targets. This will allow senior administrators to manage the process from a higher level and keep the board informed.
After the context is established and the risks identified, analyzed and evaluated, the work begins on how best to treat these risks. It must be admitted that the first parts of the process can be very interesting, and even exciting, as bringing together various departments and stakeholders into the process can feel quite satisfying. But now comes the part where those departments who had a little bit of fun identifying if quantifying the risks are upon to report their work to date and come up with a plan for formulating the future treatment of any risks assigned.

Below are some tips for implementing a formal ERM process with very little cost and without adding an enormous workload to the General Counsel, CFO, risk manager, or internal auditor. One of the greatest impediments to getting things started is the perceived enormity of the process, but these suggestions can help the ERM champions within the organization to understand that the vast majority of the work will be performed by others and that their role is predominantly oversight and cheerleading.

1. Assignment of Risk Owners -
   The only way for senior administrators to adequately manage the process is to push accountability down the organization to people with the abilities and subject matter expertise to oversee the treatment of a risk. That “risk owner” may further delegate certain tasks to others, but they must remain ultimately accountable and responsible to report their activities back to senior management. Establishing an ERM committee is highly advisable, but senior management must be prepared to keep the process moving.

2. Need for a System -
   This process of risk owner assignment and reporting takes a system. Even some very sophisticated institutions will use spreadsheets, but there are reasonably-priced, web-based platforms available that allow for the cataloging, delegation and reporting of risks. Senior administrators would then have access to check on progress and produce reports suitable for the board level.

3. Best Practice Resources -
   In today’s connected world, and given the continued collegiality among higher education institutions, best practice examples among our peers abound and are often easy to find with a simple web search. The University Risk Management and Insurance Association (URMIA), also has a library of best practices for their members as well as the ability to post questions to their community discussion forum. For those members of United Educators, they also provide an extensive library of well-researched white papers.

4. Reporting of Activities and Success -
   Any ERM program must include reporting up through the institution and eventually to the board level. Risk owners should regularly be letting senior management know their agendas and their progress toward agreed targets. This will allow senior administrators to manage the process from a higher level and keep the board informed.
5. Accountability.
   One of the most common reasons for an ERM program to languish is the lack of accountability for risk owners to keep the process moving. If no one is asking for reporting and there is no feeling on the part of the risk owners that this is important to the institution, the process is destined to die a slow death. A good system, however that is structured, is key to keeping everything moving forward.

While the reviewing of a list of representative higher education risks has the potential to stifle creativity in the institutional risk identification process, below is a sample of risks common to a college or university for reference. The list should not be shared with those you have asked to participate in risk identification sessions, but can be helpful to the ones with overall responsibility to ERM implementation to see if anything glaring might be missed.

### Sample Enterprise Risk Portfolio

<table>
<thead>
<tr>
<th>Revenue Protection</th>
<th>Financial Stewardship</th>
<th>Emergencies &amp; Crises</th>
<th>Compliance &amp; Reporting</th>
<th>Employment Issues</th>
<th>Student Issues</th>
<th>Data Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Academic Reputation</td>
<td>Treasury Risk Controls</td>
<td>Campus</td>
<td>NCAAs</td>
<td>Background Checks</td>
<td>Student Mental Health</td>
<td>Personally-Identifiable Informatio n Breach</td>
</tr>
<tr>
<td>State &amp; Federal Support</td>
<td>Financial Audits</td>
<td>Violence</td>
<td>OSHA</td>
<td>Training</td>
<td>Student Discipline</td>
<td>External Attacks</td>
</tr>
<tr>
<td>Grants &amp; Contracts</td>
<td>Internal Audit</td>
<td>Residence</td>
<td>EPA</td>
<td>Faculty/Staff Retention</td>
<td>Alcohol &amp; Drug Abuse</td>
<td>Employee Malfeasanc e</td>
</tr>
<tr>
<td>High School Graduate Demographics</td>
<td>Fraud</td>
<td>Hall Fire</td>
<td>FERPA</td>
<td>Executive Succession</td>
<td>Assaults &amp; Other Violence</td>
<td>Operational Interruption</td>
</tr>
<tr>
<td>Economic Conditions</td>
<td>Debt Management</td>
<td>Safety</td>
<td>Clery Act</td>
<td>Safety</td>
<td>Academic Dishonesty</td>
<td>Lost or Stolen Media</td>
</tr>
<tr>
<td>Academic Program Demand</td>
<td>Insurance Protection</td>
<td>Natural Disasters</td>
<td>HIPAA</td>
<td>Wellness</td>
<td>Experiential Learning</td>
<td>Trade Secrets</td>
</tr>
<tr>
<td>Student Quality</td>
<td>Physical Asset Protection</td>
<td>Pandemic</td>
<td>Workers' Compensation</td>
<td>Tenure</td>
<td>Bullying &amp; Cyberbullying</td>
<td></td>
</tr>
<tr>
<td>Response to Changing Academic Delivery</td>
<td>Government Compliance</td>
<td>International Incidents</td>
<td>FMLA</td>
<td>Administration</td>
<td>Hazing</td>
<td></td>
</tr>
<tr>
<td>Media Exposure</td>
<td>Environmental Sustainability</td>
<td>External &amp; Internal Threats</td>
<td>ADA</td>
<td>Discrimination</td>
<td>Social Media</td>
<td></td>
</tr>
<tr>
<td>Athletic Success</td>
<td>Public Relations</td>
<td>Public Relations Response</td>
<td>NLRB</td>
<td>Sexual</td>
<td>Employee Misconduct</td>
<td></td>
</tr>
<tr>
<td>Development Relations</td>
<td>Business Continuity</td>
<td>Business Continuity</td>
<td>Title VII</td>
<td>Harassment</td>
<td>Alcohol &amp; Drug Abuse</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Title IX</td>
<td>Reductions in Force</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>HEA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>FCRA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Funded Research</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Graham Leach Biley</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>PC!</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>.....</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The National Association of College and University Attorneys
IV. The Hottest of Hot Compliance Topics for Today and Tomorrow

Then and Now

A. Then:

1. Focus then: Why Compliance?

   a. To have an effective compliance and ethics program, colleges and universities had to exercise due diligence and promote a culture that encouraged ethical conduct and a commitment to compliance with the law.
   b. The program had to be reasonably designed, implemented, and enforced so that was generally effective in preventing and detecting criminal conduct.
   c. Specific individuals within the school had to be delegated day-to-day operational responsibility (N.B. The term "Compliance Officer" is not used) and had to report periodically to high level personnel and, as appropriate, to the governing body.
   d. Effective training programs had to be conducted and information disseminated.
   c. Periodic evaluations of the program had to be conducted by the school.
   f. A mechanism such as a "hot line" had to be established to allow employees to report confidentially potentially criminal conduct.
   g. Appropriate response to criminal conduct with corrective action was necessary.

3. Variations on the theme: The Guidelines formed the foundation for many other federal agency guidance. For a comprehensive list of the DHHS ones, which also impact NIH-funded research grant recipients, see. http://oig.hhs.gov/compliance/compliance-guidance/compliance-resource-material.asp. While most of the resource materials are directed at corporate responsibility for health care entities, the guidance is equally applicable to the higher education sector, especially "Corporate Responsibility and Corporate Compliance: A Resource for Health Care Boards of Directors," April 2, 2003: http://oig.hhs.gov/fraud/docs/complianceguidance/040203CorpRespRaceGuide.pdf

4. Compare and contrast:
   a. Rules-based compliance v. values-based compliance
      Rules-Based Compliance: In its more limited meaning, compliance is doing that which you are required to do. It's this form that often generates a negative connotation among university personnel because it is predicated on rules, oversight and enforcement activities. The compliance department is just as much "the enemy" as is the outside enforcement agency.
   b. Values-Based Compliance System: Further to the right on the compliance model continuum and closer to "best practices," the values-based compliance structure often connects codes of conduct and ethics structures to the institutional mission

---

1 See, 2008 NACUA Annual Conference outline, "Compliance: A Practical Protocol for the Entire Campus (And Beyond)," presented by Thomas A. Butcher and William R. Kaufman

2 Id. for a complete description of the requirements of that statute.
statement with a focus on creating a supportive climate for "doing the right thing." While more labor intensive to develop because of the need to engage the university community in a culture change, the values-based system moves the institution away from the "compliance for the sake of compliance" model to a system featuring greater employee acceptance, understanding and support.

c. Organizational structures for supporting compliance: Best thinking then and now.

d. Northern Illinois University - Compliance Administration jointly reports to the Vice President and General Counsel and acting Executive Vice President of Finance & Facilities/Chief of Operations.  
http://www.niu today.info/2013/03/12/niu-to-fortify-compliance-administration/

e. University of Kansas- Director of Institutional Compliance provides independent oversight and coordination of an institutional compliance program. The Director reports to the Institutional Compliance Executive Committee, which includes the Chancellor, Provost, and five senior administrators (including the General Counsel), with day-to-day supervision provided directly by the Senior Vice Provost for Academic Affairs (and also via a "dotted line" by the General Counsel).  
http://provost.ku.edu/sites/provost.drupal.ku.edu/files/docs/provost_office_org_chart.pdf

f. Grand Valley State University - Legal Office, Risk Management Office and Compliance Office under one umbrella that reports to the University Counsel who reports to the University President. http://www.gvsu.edu/uco/

g. University of New Mexico - Main Campus Chief Compliance Officer reports to the President and indirectly to the Board of Regents through its Audit Committee. Health Science Center Chief Compliance Officer reports to Chancellor of the Health Sciences Center. http://hsc.unm.edu/admin/compliance/

5. Best practices for establishing an institutional culture for compliance-fostering a common awareness that allows individuals to focus attention on risks with strategic impact: Best thinking then and now ... The more recent emphasis on Enterprise Risk Management (ERM) and its incorporation in institutional strategic planning is helping advance the compliance activities in a positive manner. The failure to comply is an Enterprise Risk and effective management controls are important in minimizing both the likelihood and impact of loss.

6. Queries:
   a. Who should be assessing risk?
   b. How does it fit within the institution's strategic plan?
   c. How does an institution enhance and strengthen a culture of compliance while protecting its decentralized, collaborative, entrepreneurial nature?
   d. How does an institution identify and map the inter-relation of risk factors across the institution, not functionally?
   e. Who ranks the risks, and how?
   f. What mitigation strategies and measures should be employed?
   g. Who is identifying significant gaps in the management of risk?
   h. How should all these efforts be documented?
B. Now: Hot issues: What are the new, foreseeable risk threats to a university's goals?

1. Reputational risk:
   a. Scandals, especially sex scandals or ones involving minors or assaults by institutional personnel.
      i. Freeh report fallout
      ii. Former Rutgers Men's Basketball Coach

   b. Risk only increases as more and more activities take place off campus
      i. Community events
      ii. Student work placements
      iii. Academic practicums

2. Cyber crime
   a. Hackers
   b. Social activists, disgruntled students and staff target universities

3. IT failures
   a. E.g., Saint Joseph sending out student name linked grades in error
   b. Owners of sensitive data more responsible for care of private information
   c. E.g., Distance-learning dependence
   d. Query: Does information need to be kept? Who needs access to it? Where is it housed?
   e. Query: If so, how is it being protected, what safeguards have been imposed to prevent accidental disclosure/deletion?

4. Global warming-preparation for worst weather scenarios
   a. E.g., NYU labs preparing/ not protecting animals used in experiments during and after Hurricane Sandy
   b. Machinery breakdown, freezer losses, broken pipes, injury to students and staff

5. Risks imposed by the federal government
   a. Exit of leaders within Department of Education with institutional history/knowledge means novice enforcers auditing a campus operating with a lack of context to determine if violations, significant or not, have occurred
   b. E.g., Audits to determine compliance with April 2010 Dear Colleague letter re Title IX
   c. Audits to determine compliance with the ever expanding reach of the Clery Act and additional requirements to break out data even more
      i. Virginia Tech’s continuing challenge to fines imposed by the federal government
   d. E.g., Violence Against Women Act additions
   c. E.g., The Drug-Free Schools Act expansion

6. Risks imposed by the NCAA
   a. Reliance on precedent may not be a reliable indicator of NCAA reaction to significant misconduct in at least one significant situation—one-off decisions
   b. E.g., Penn State penalties
7. Risks created by new ways to deliver education
   a. Compliance with state authorization statutes
   b. Privacy and quality issues
   c. Questions about need for higher education as it exists today

Bottom line: What is the best way to provide enterprise risk management?

V. The New Language of Risk- What Every Higher Ed Institution Should Know About Enterprise Risk Management (By Dorothy Gjerdrum, Arthur J. Gallagher & Cos.)

Although there were no newspaper headlines, parades or tweets announcing its arrival, in November of 2009, the paradigm for how we manage risk changed. This change was more than five years in the making, and experts from around the world contributed to its creation, including an advisory group from the U.S. The effort was coordinated by the International Organization for Standardization (ISO). The international standard on the practice of risk management (ISO 31000) was published along with two companions: a definitions guide (Guide 73) and guidance on the assessment of risk (ISO 31010). ISO 31000 was immediately adopted as the American standard on risk management by the American National Standards Institute (ANSI). The new language of risk, and how to implement an enterprise-wide approach to risk management, is described in that standard and outlined here for your consideration.

The ISO framework provides an accessible and practical approach to managing risk broadly across an organization. It is grounded in the value that risk management can bring to an organization- whether public or private, small or large. And the standard recognizes that risk can be both good and bad; which acknowledges that when we are aware and ready, risks are worth taking. This is very good news for people who manage risks in colleges and universities in this ever expanding world of risk in which we operate.

The truth is, risk is present in everything that we do. Faculty, employees and students manage risk all day long, whether they realize it or not. The enormity of the challenge is driven home when we bear witness to a campus shooting or a catastrophic weather event or a sleepy van driver that rolls off a highway. But our institutions are also challenged by ordinary, daily occurring threats such as workplace injuries, cyber attacks and vandalism. If we don’t understand the importance of managing all risks, we can get caught up reacting to the most scandalous or highly publicized risks at the expense of the frequent and common. And if we don’t have everyone engaged in managing risk, then we may overlook risks that are known but not effectively communicated (think of sexual misconduct cases, where someone always knows - or should have known).

We need to think about risks beyond insurable risks, as well. People can get caught in the trap of thinking “I don’t have to worry about that. That’s what insurance is for.” When questioned, insurance companies estimate that only 20-30% of all risk exposures are insurable. The ways we treat and manage risk need to go well beyond an insurance solution. We are also increasingly subject to global risks- no matter where we live. Events in recent years have raised our awareness of our global interconnectedness for risks such as pandemic flu, cyber attacks and

The National Association of College and University Attorneys
economy and supply chain risks. Now more than ever, we need everyone to increase their **risk awareness**.

In 2010, the National Standards Association of Ireland published an implementation guide to ISO 31000 and it states that: “The purpose of managing risk is to increase the likelihood of an organization achieving its objectives by being in a position to manage threats and adverse situations and being ready to take advantage of opportunities that may arise.” [www.n sai.ie](http://www.n sai.ie) To translate that for higher education institutions: Colleges and universities need to know the new paradigm for managing risk in order to support the achievement of their objectives by managing potential threats and taking appropriate risks.

The ISO standard defines **risk** as the "effect of uncertainty" on an organization's objectives. Every institution has objectives; they are your highest expression of intent and purpose.

There is a lot of uncertainty in the world; it results from unknown conditions, causes and sources that are often beyond our direct control. When that uncertainty affects your institution's ability to achieve its objectives, that uncertainty becomes "risk." Risk is anything that could harm, prevent, delay or enhance your ability to achieve your objectives. Stated another way, risk is **not** just an event, consequence, likelihood, vulnerability, hazard, threat or opportunity but rather the effect of those upon your objectives. Let's assume that continuing operations post disaster and effective crisis response are key objectives for a college. Therefore, a tornado is a hazard that creates risk only if the college is not ready to respond to the effect of the tornado upon operations.

The standard also recognizes that sometimes "taking a risk" is appropriate and the standard provides a framework and process that supports the opportunities inherent in taking risks.

**The Evolution of Risk Management**

The evolution of how we manage risk in the U.S. has been expanding over the past few decades; the ISO standard helps us move that practice to a more strategic approach. The risk management structure of 10 and 20 years ago is not as effective or forward thinking. For example, risk is not always bad, and it is not fully addressed through the purchase of insurance. Far too often, risks have been managed in "silos" with workers compensation, emergency planning and insurance purchase each led by separate people within the organization, with little overlap or cross coordination. Most colleges and universities employ a variation of the middle column, a more integrated approach to managing risk. It is not a bad approach, but it is not as forward thinking or broad as an enterprise-wide approach.

Implementing ISO 31000 can help an organization move to a more strategic approach. The standard outlines a broader approach to risk, one that engages people at all levels of an organization, working within a **common framework**.
**Transactional Risk Management**
- Purchase insurance to cover risks
- Hazard-based risk identification and controls
- Compliance issues addressed separately
- Safety & emergency mgmt handled separately
- RM is not integrated across organization
- Risk Manager is insurance buyer

*Risk is bad* - focus is on transferring risk

**Integrated Risk Management**
- Greater use of alternative risk financing
- More proactive about preventing and reducing claims
- Integrates claims mgmt, contract review, special eventRM, insurance and transfer techniques
- Cost allocation used for education and accountability
- More collaboration -as dept's are willing
- Risk Manager may be the risk owner

*Risk is an expense* - focus is on reducing Cost of Risk

**Enterprise-wide Risk Management**
- A wide range of risks are discussed and reviewed, including reputational, financial, strategic and operational
- Aligns RM process with strategy and mission
- Broader definition of "risk" to include opportunities; focus on uncertainty
- Helps manage growth, allocate capital & resources
- Risks are owned by those who control them
- Many risk treatment & analytical tools available
- Risk Manager is facilitator and leader

*Risk is uncertainty* - focus is on optimizing risk to achieve goals