Enterprise Risk and Compliance Management
Their Integral Roles in Higher Education Governance
Introduction

Anyone involved in the management of higher education institutions in the United States will not normally make it far into a conversation with colleagues without the topic of enterprise risk management or compliance making its way in. There is mounting pressure from governing boards to be assured that risks surrounding the strategic mission of the organization, including the risks of noncompliance with an ever-growing list of laws and regulations, are being identified, measured and treated.

But the next question is normally, “How in the world can I even begin given the already-stressed resources of our institution?” A university general counsel recently told the story of how she would wake in the middle of the night worried about a recent news story highlighting a particular risk facing colleges and universities. When she arrived at work the next morning she would figuratively pull risk and compliance out of her drawer and put it on her desk to begin considering where to start. Then, after many days of looking at the stack in front of her, and with thankfulness for a shortage of news events to support her original fear, she slipped the stack back in the drawer where it was safe until the next, inevitable sleepless night.

This counsel, as well as any number of higher education risk managers, are not alone. Enterprise risk and compliance management often looks to be a task too formidable to even consider beginning. However, there are many models and tools, to be explored later, which can help make the journey both possible and perhaps even enjoyable.

Defining Enterprise Risk and Compliance

Enterprise Risk Management

The term enterprise risk management (ERM) is somewhat unique to the U.S. In most of the world, when the more general term “risk management” is used, it is the broader view of risk that we call ERM that is intended. In this country though, ERM has become a helpful differentiator from what we now might call traditional risk management (TRM), or the well-polished functions of risk financing, loss control and claims management. This discipline of TRM has saved U.S. corporations and nonprofits billions of dollars and helped keep countless workers, customers, students and the public free from harm, and we are many strides ahead of the rest of the world in this area.

The principal difference between ERM and TRM, however, can be found in how risk is defined. Traditional risk is defined by Merriam Webster as, “the possibility that something bad or unpleasant will happen” and risk management is defined by The Institutes as, “minimizing the adverse effects of accidental losses.” Both definitions of risk and traditional risk management foresee only harm and our job is then to minimize its adverse effects.

ERM takes a broader view. ISO 31000, the international risk management standard, defines risk as, “the effect of uncertainty on objectives.” This definition is not limited to traditionally insurable risks. In fact, less than ten percent of the items on a typical ERM risk register can be insured. Instead, the majority of risks identified are tied to the mission and objectives of the organization.

RISK can be a threat or opportunity

Anything that can harm, prevent, delay or enhance an organization’s ability to achieve objectives = RISK

ERM delineates the threats that could keep the institution from achieving its objectives and looks for any and all opportunities that could be exploited to increase the likelihood of those same objectives being realized.

In Janice Abraham’s book entitled, Risk Management: An Accountability Guide for University and College Boards (AGB Press, 2013), she offers a helpful definition of ERM as, “a business process led by senior leadership that extends the concepts of risk management and includes:

- Identifying risks across the entire enterprise;
- Assessing the impact of risks to the operations and mission;
- Developing and practicing response or mitigation plans; and
- Monitoring the identified risks, holding the risk owner accountable, and consistently scanning for emerging risks.”

Enterprise Compliance Management

Although the phrase enterprise compliance management (ECM) has not yet embedded itself into our corporate lexicon, it is a helpful way to look at how compliance could be managed—on an enterprise-wide basis rather than in departmental silos as is the case in most colleges and universities. There has certainly been some debate about whether compliance is a part of ERM or should stand on its own in the higher education environment, but the conventional
Wisdom seems to be leaning heavily toward making the risk of noncompliance with applicable laws, regulations, industry codes and organizational standards an integral component of managing the institution’s overall risk profile.

Peter Lake, Professor of Law and Director of the Center for Excellence in Higher Education Law and Policy at Stetson University College of Law, identified in an article entitled, Welcome to Compliance U: The Board’s Role in the Regulatory Era in the July/August 2013 edition of Trusteeship Magazine, that higher education institutions should:

- “Recognize that regulatory compliance is a major institutional challenge and a source of both risk and opportunity.
- Strongly avoid direct operational management of critical compliance issues from the governing-board level.
- Promote an enterprise risk management (ERM) approach. That includes encouraging the creation of a centralized ERM function with leadership that reports directly to the board and making sure that there are processes in place for establishing important compliance policies and keeping them up to date.
- Ensure that the institution coordinates compliance initiatives throughout the campus as part of ERM efforts. The organizational chart should clearly identify the office and individuals tasked with such coordination.”

In December 2014, ISO issued a new standard for compliance management (ISO 19600) which takes an enterprise and risk-based approach which naturally brings compliance together with ERM and congruent with the principles, framework and process outlined in ISO 31000. Both standards are tied to identifying and treating threats and opportunities in a manner that best preserves the meeting of organizational objectives. In that way, compliance risk is defined similarly as the broadened view of risk we see as part of ERM and both are managed using comparable processes.

DEFINITIONS OF RISK

<table>
<thead>
<tr>
<th>Traditional</th>
<th>Broadened</th>
<th>Compliance Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>The possibility that something bad or unpleasant will happen.</td>
<td>The effect of uncertainty on objectives.</td>
<td>The effect of uncertainty on compliance objectives.</td>
</tr>
<tr>
<td>Merriam-Webster</td>
<td>ISO 31000</td>
<td>ISO 19600</td>
</tr>
</tbody>
</table>

“Risk is often expressed in terms of a combination of the consequences of an event and the associated likelihood of occurrence.”

“Compliance risk can be characterized by the likelihood and the consequences of noncompliance with the organization’s compliance obligations.”

Risk and Compliance as Part of Higher Education Governance

One of the primary inhibitors to the implementation of enterprise risk and compliance management throughout the college and university environment is the misunderstanding of where these disciplines fit within the organization. Many institutions have started and then found their programs languishing because they have been managed in silos, almost as separate operational functions of the organization. The method called for in ISO 31000 and 19600 is for the institution to see risk and compliance as integral pillars of the overall governance of the college or university.

In a paper published in 2014 by the Association of Governing Boards of Universities and Colleges (AGB) and United Educators (UE) entitled, A Wake-Up Call: Enterprise Risk Management at Colleges and Universities Today, it was suggested that, “Risk management, at its core, is a governance and management discipline, not an end but a means to the end, with the end being the accomplishment of the institution’s mission. Boards and administrators need to take demonstrable action and advance ERM efforts at their institutions.
There is no choice: each institution and board needs a process by which it routinely identifies, evaluates, and plans for risks that have the greatest potential for reputational injury or obstruction of institutional mission. Risk offers opportunities to lead change, and institutions and boards need plans and processes in place that allow them to assess that risk and take advantage of those opportunities when they arise.”

Risk, including compliance risk, are therefore elevated out of what has been the functional mindset in higher education to a seat at the table within the governance structure of the institution. This seat is alongside, and in support of, mission, strategy, stewardship and quality, with audit and assurance as the final piece. Each has its role in making sure that the direction of the governing board is realized:

---

**Centralized Oversight-Decentralized Implementation**

One of the most frequently asked questions about enterprise risk and compliance management is, “How do I get started given the scarce resources and daily pressures at my institution?” The answer lies in a model described by many as Centralized Oversight-Decentralized Implementation. Jeff Chasen, Associate Vice Provost for Institutional Compliance at the University of Kansas, has been using this method since 2013. He states, “I have found that our ability to bring change to the institution has been greatly influenced by the utilization of a model that allows for the compliance office to remain the central organizer, gatherer, facilitator, and resource. We maintain our structure with responsibility for specific compliance functions assigned to the subject matter experts within our units, a role many of them held long before we began to formalize our program. Our centralized office facilitates the development of strategic action plans, coordinates (and serves on) working groups, fosters additional collaboration and resources, tracks progress, reports to senior leadership, and helps brings heightened accountability to the process.”

Both the ISO 31000 and 19600 standards advocate for a centralized oversight and decentralized implementation approach which takes advantage of risk and compliance obligation owners throughout the institution. These owners will develop treatment plans, normally with the oversight and
direction of a risk committee, manage the risks and compliance obligations and report progress upward within the organization.

The ISO standards are filled with helpful details for implementing a successful enterprise risk and compliance management program. They provide the architecture, but are scalable and tailorable for any college or university, no matter the size or complexity.

ISO 31000 (risk) and ISO 19600 (compliance) provide the Architecture Scalable and Tailorable

The essence of ISO 31000 and 19600, taken together, is simply:

1. Know your risks and compliance obligations through identification and evaluation, making sure you consider the context and stakeholders.
2. Manage the risks and compliance obligations through delegation and placing ownership with subject matter experts.
3. Provide for central oversight, accountability and reporting.
4. All using a risk management framework established by senior leadership with built in monitoring, review and continuous improvement.

What Makes Enterprise Risk and Compliance Management (ERCM) Work?

Doug Huffner, the Senior Director and Chief Risk Officer for The Ohio State University stated that, “When we first began our URM (University Risk Management) program in 2013, I could not have imagined the value proposition that was about to transcend our institution. What started out as mostly defensive and guarded discussions of threats and barriers to achieving the University mission, quickly and completely turned around into a robust conversation about opportunities and strategic planning. Our senior-level risk committee meetings are lively and well-represented. It is amazing how our cross-functional committee, while staying focused on our risk and compliance-based decisioning model, is driving real innovation and progress throughout the University.”

Somewhat counterintuitively, taking an enterprise approach to risk does not make the organization more risk averse, but has the opposite effect. The Ohio State story is not unique. ERCM, done right and with the right tone, will actually help create and maintain an environment of innovation and risk taking. If a process is in place to carefully consider the risks of new ventures, a more informed decision will be the result. And when the venture is ready for launch, it will be with much greater confidence and with the desired outcome more sure.

There are many reasons why ERCM works and why it makes colleges and universities better:

1. Focuses on mission and objectives—Everything is tied back to the central purposes of the institution and efforts are prioritized accordingly.
2. Preserves and creates value—A dynamic ERCM program will both preserve what is already going well and create new opportunities to advance the institution into the future.
3. Emboldens innovation—Clearly identifying risk and agreeing on treatment plans to bring any residual risk under control, frees leadership to take more risk in support of innovation.
4. Enhances agility and resilience— By having risk and compliance under control throughout the institution, the organization can be ready much more quickly to respond to opportunity and the possibility of a threat having irreparable harm is greatly reduced.
5. **Formalizes process and governance**—Having risk and compliance embedded as pillars in the governance model will keep these disciplines in the forefront whenever decisions are made and when management tools are reviewed and developed.

6. **Improves quality of decisions**—When risk and compliance is at the table, any decision-making process will be improved—less risk of threats and more opportunities exploited will be the result.

7. **Helps in allocation of resources**—As the institution makes decisions about the allocation of limited resources, taking a risk-based approach will enhance the organization’s ability to move funds where they best reduce institution-wide threats and enhance opportunity.

8. **Improves stakeholder confidence and trust**—The ERCM process gives internal stakeholders (e.g. board, faculty, staff, students, families, donors, alumni) and external (community, government, accreditation bodies, creditors, rating agencies) greater assurance that their investment in, fidelity to, and reliance on the institution is warranted.

9. **Empowers subject matter experts**—ERCM improves both overall organizational productivity through delegation and gets the work to the person with the best education and experience to inform the issue.

10. **Everyone’s a risk manager**—A comprehensive and ever-improving ERCM program will undoubtedly begin to change the culture of the institution, making risk and compliance a consideration in everything it does, at every level.

**Governance, Risk and Compliance Software**

There are several vendors offering software packages for institutions to manage their risk and compliance programs using either cloud or server-based packages. Features common to many of the platforms include:

- Detailed risk and compliance obligation registers with multiple data points
- Dashboards for each risk and obligation with the ability to rank risks and catalogue treatment plans
- Risk rankings that flow into interactive, institutional heat maps
- Ability to manage delegations using email assignments and workflow through calendars
- Reporting tools for use at all levels of the organization, including the board

These systems can be very helpful in the management of a complex enterprise risk and compliance management program and are generally cost-effective.

**Conclusion**

The importance of risk and compliance management at institutions of higher learning cannot be underestimated. They fill in two critical components of governance and are among the most important means by which any organization will increase the likelihood of achieving its mission and objectives.

**WHY IS RISK AND COMPLIANCE MANAGEMENT IMPORTANT?**

1. All organizations exist to achieve their objectives.
2. Many internal and external factors affect those objectives, causing uncertainty about whether the organization will achieve its objectives.
3. The effect this uncertainty has on an organization’s objectives is “risk” or “compliance risk.”

In summary, the management of risk, including compliance with relevant laws, regulations, industry codes and organizational standards, is central to the livelihood and success of all organizations.

There are no greater institutions in our nation as our colleges and universities in the way they contribute to our health, our economic prosperity and help form tomorrow’s generations. Assuring the fulfillment of their collective vision and securing their future is a worthwhile and necessary pursuit.
About the Author

Scott Wightman is an Area Executive Vice President for Arthur J. Gallagher & Co. and serves on the national leadership teams of their Higher Education and Enterprise Risk Management Practices. He is a former corporate risk manager and Director of Risk Management for Saint Louis University. He is also an active member of the University Risk Management and Insurance Association (URMIA) and serves as a member of the faculty for the PRIMA/URMIA ISO 31000 training program. He was awarded the 2014 Power Broker Award in Education from Risk & Insurance Magazine and the 2015 Innovation Award from Business Insurance. He holds the ARM-E designation from The Institutes for Enterprise-Wide Risk Management.

For more information, contact:

Scott Wightman, ARM-E
Gallagher Higher Education Practice
scott_wightman@ajg.com