LEVERAGING ENTERPRISE RISK MANAGEMENT: Opportunity for Greater Relevance

By Janice M. Abraham, Robert Baird, and Frank Neugebauer

Enterprise Risk Management (ERM) gained a foothold in higher education during the first decade of the 21st century. College and university governing board members came to their board service with the perspective and experience of having served on corporate boards and in corporate leadership positions where ERM was in active use. Trustees asked senior leaders at colleges and universities to begin ERM programs. As a result of these requests and financial pressures, public and private institutions are now implementing ERM business processes to support strategic and annual planning and also analyses of major new initiatives. Institutional leaders are evaluating not only the downside of risk (i.e., what could go wrong) but also the upside—the opportunities presented by taking on additional risk.
Information technology is so integral to the mission and operations of colleges and universities that it regularly tops the list of risks for boards and senior leadership. This means that even though ERM engages the entire higher education institution, IT organizations have an opportunity to use ERM to move beyond a services function toward providing strategic value to the institution. By understanding the business of higher education, communicating with various units and departments, and leveraging ERM, the IT organization can lead as never before.

Understanding and Analyzing Risk
ERM is a process that identifies, prioritizes, manages, and communicates those risks that have the potential to prevent an institution from realizing its goals—for example, risks that can impact a capital campaign, an international program, or a new online degree. Allocating resources to manage the risks in the right places allows campus administrators to spend their limited resources on the things that are critical to the institution's mission and to the achievement of its plans. As noted, there are both downsides to unexpected risks (yes, bad things happen) and upsides (rewards when something positive happens). For example, the Internet's effects on education were not immediately understood in the 1980s, but as the Internet evolved, institutions were able to properly (and constantly) monitor both the unexpected risks (e.g., viruses) and the unexpected rewards (e.g., online learning).

ERM should be a part of every higher education institution's planning and operations. The discipline of ERM supports an institution's ability to evaluate risks and opportunities and to focus scarce resources on institutional priorities. As a process, ERM is not a project that is completed in a defined time period. ERM is best incorporated into the regular institutional budget and planning processes so that risk-mitigation strategies can be integrated into the annual plan with appropriate funding and support. Strategic planning and capital planning offer other opportunities for institutions to adopt the ERM process. Risk management and IT professionals can work with internal auditors to coordinate and not duplicate initiatives.

Four Steps of ERM
ERM consists of four steps:
1. Identify risks: create a risk register.
2. Assess the likelihood of risks and their impact on the institution.
3. Develop a risk management plan.
4. Measure, track, and communicate risks.

ERM Step 1. Identify Risks: Create a Risk Register
The ERM risk register is a view of the most essential risks facing an institution—the risks that, if they occur, could prevent the institution from achieving its goals and objectives. The purpose of the register is to maintain focus where it belongs: on those risks.

An institution can maintain different risk registers for various levels of the institution's leadership hierarchy. From the governing board to senior IT management to mid-level IT management, each level provides relevant insight. For instance, operational IT matters do not appear on a board-level risk register, just as strategic initiatives do not appear on a department supervisor's risk register. However, each level expands to the level above it, providing cohesion throughout. An added benefit of such registers is to help individuals understand their role in ERM—that is, the level of detail at any given level should make roles clear.

Best practice for an ERM risk register includes maintaining lists of no more than ten enterprise risks to help identify, assess, and manage risks at the appropriate level of scope and control. The sample risk register questions below are a good place for institutions to begin, adapting the questions to fit individual institutional priorities.

Governing Board Risk Register Questions
1. IT strategy. Does the IT strategy reflect the institution's core values and strategic plan?
2. Protection. Do agreements with partners properly protect intellectual property rights and other institutional values (e.g., privacy and nondiscrimination)?
3. Privacy. Does the IT organization regularly assess changes in privacy laws and other federal and state compliance areas?
4. Security. Does the institution perform regular IT security risk assessments and report its findings to the board?
5. Missed opportunities. Is the institution taking enough risk with its IT strategies? Are there opportunities, perhaps ones that would enhance the educational experience, that have not been considered?
6. **Succession planning.** Is there a succession plan in place for all key IT personnel?

Table 1 shows this risk register. Note that the register in Table 1 does not ask questions but notes elements of risk, which are then rated.

**Senior IT Management Risk Register Questions**

1. **Data analytics.** Does the institution regularly use data analytics in the decision-making process?
2. **Mobile platform.** Is the institution developing a strategy to support a mobile teaching and learning strategy?
3. **Business continuity.** Does the IT organization have a business continuity plan, and is it tested periodically?
4. **Systems and data security.** Does the IT organization have and regularly execute a plan to test critical systems to prevent data breach and inappropriate information sharing from internal and external sources? Is an external security expert used for such testing?
5. **Best practices.** Are IT standards—those from best practices as defined by various organizations such as ISO, ITIL, and SAS—followed?
6. **Contracts.** Are contracts with service providers designed to include protections that the institution desires (e.g., uninterruptable service)?

**Mid-Level IT Management Risk Register Questions**

1. **Training.** Is appropriate training in place for IT staff? Does the training extend to the campus community to maximize operations of IT equipment?
2. **Internal audit.** Has an audit plan been created and executed to ensure that key IT development and operations processes are conducted consistently?
3. **Infrastructure.** Are all networks highly available and redundant? Are server room cooling and fire-suppression systems maintained?
4. **Data security.** Are security patches applied to operation systems, applications, and appliances? Is an e-mail archiving system in place? Is institution staff periodically trained in desktop security policies and procedures? Are desktop resources physically secure? Are server rooms secure and restricted to authorized staff only? Do mobile devices have adequate password and encryption established to prevent loss of data should a device be lost or stolen?

### TABLE 1. BOARD-LEVEL IT RISK REGISTER

<table>
<thead>
<tr>
<th></th>
<th>Urgency Rating</th>
<th></th>
<th>Person To Address (if rated “1”)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Intellectual property agreement</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Privacy compliance</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security risk assessment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Missed opportunity assessment</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Succession planning</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Additional Board Governance Risk Areas:**

5. *Litigation.* Have IT staff been trained in implementing litigation holds for potential lawsuits and in participating in electronic discovery during litigation?

Identifying and managing future risk is not a matter of clairvoyance. Rather, it involves the diligent exercise of watching what’s happening elsewhere. For information technology, regularly following Twitter feeds, CSS feeds, EDUCAUSE programs, and non-IT news sources can provide valuable insight into emerging trends. Similarly, some “emerging” sources of risk occur within the organization. IT professionals should stay involved in teaching, research, and service planning to ensure early identification of IT risks and opportunities supporting these programs. When IT leadership is involved early, ERM can be integrated into program planning. In this way, the risk register becomes an integral process rather than an afterthought. In addition to involving IT leaders in early program planning and risk identification, sending a quarterly report on emerging risks to the appropriate members of the community (e.g., the president’s cabinet or other senior-level team members) is a best practice.


Following the compilation of risk registers, management teams can rank the risks based on the likelihood (probability) that the risk will occur and on the potential impact if the event occurs. Using a simple map, such as a heat map (see Figure 1), managers can identify the risks with the highest likelihood and biggest potential impact, focusing the team’s attention on developing mitigation plans for these risks while working down the list of the priorities over time. Calculating a risk score and risk appetite or tolerance helps to focus and prioritize mitigation efforts.

Figure 1 shows that the risks of student enrollment and management turnover require additional attention but that the risk of disaster recovery and business continuity requires less. Note that this heat map is not detailing the risks in a general sense; they are specific to the institution. This means, for

**Figure 1. Sample Heat Map of a State System**

1. Student enrollment
2. Management turnover
3. Governance
4. Government support
5. Health care costs
6. Employee morale
7. Disaster recovery and business continuity
8. ROI in new initiatives and capital projects
9. Information security
10. Liquidity
11. Legal/regulatory compliance
12. Potential for fraud and conflicts of interest

example, that although the disaster recovery and business continuity risk is worth significant attention within ERM, a particular institution may be well prepared.

**ERM Step 3. Develop a Risk Management Plan.**

Identifying and assessing risks are important first steps in ERM, but studies reveal that campus professionals spend the majority of their time on these two steps, neglecting the more critical steps of mitigation and monitoring. There are four paths that risks can take within a risk management plan:

1. The initiative or cause of the risk is eliminated because it's simply too risky.

2. The risk is transferred to or shared with other entities. This can occur by establishing a partnership with appropriate contracts to meet the objective (e.g., if online courses are a critical part of an institution’s strategy, partnerships with marketing companies and learning management system vendors can reduce the risks of new ventures). Or an institution can purchase insurance to reduce the risk (e.g., cyber liability insurance can facilitate compliance with state consumer-protection laws).

3. The risk is accepted, but changes are made to reduce the risk (e.g., increased investments in training and oversight are made or additional security is added to reduce identified risks).

4. The risk is accepted, and no additional changes are made to reduce the risk.

Although the disaster recovery and business continuity risk is worth significant attention within ERM, a particular institution may be well prepared.
IT leaders bring a risk management perspective not otherwise present in an institution, but such perspectives can be lost in the jargon and technical nuance, which is why it is critical for IT leaders to learn, comprehend, and speak in the language of the institution. The best IT opinion stated in IT terms can be lost if the recipient does not understand the jargon or the subtleties.

Risk management plans—especially the details within the plans—show what is being done to deal with risks (i.e., what changes are being made to either minimize or maximize risk). Soliciting a wide variety of expert (and non-expert) opinions on a risk can help to create meaningful changes. It is important to remember that change is not intended to simply reduce risk; some changes are meant to fully realize the positive impact of taking a risk. An example is the institutional use of credit cards. If the IT organization were to suggest using only paper transfers instead of online, onsite POS (point of sale) and revolving card readers, the maximum value of taking the risk would be lost. Maximizing the value of the risk also comes with increased consequences. Providing a comprehensive view of institutional changes to maximize value and minimize risk is a key factor in managing risks and is an important point of the risk management plan.

**FIGURE 2. RISK MANAGEMENT REPORT FOR THE BOARD**

<table>
<thead>
<tr>
<th>Date:</th>
<th>Jan. 1, 20xx</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of Risk:</td>
<td>Enrollment</td>
</tr>
<tr>
<td>Accountability:</td>
<td>Vice President, Admissions and Financial Aid</td>
</tr>
<tr>
<td>Board Committee:</td>
<td>Student Affairs</td>
</tr>
<tr>
<td>Description of Risk:</td>
<td>Applicant pool, admit rate, and yields all producing negative trends. High school graduates in tri-state region declining. Graduation rates below peer institutions.</td>
</tr>
</tbody>
</table>

| Likelihood: | 4 (rate 1 – 5) |
| Impact:     | 5 (rate 1 – 5) |
| Risk Score: | 20 (likelihood x impact); Level 4 |
| Risk Tolerance: | Level 3 |
| Treatment/Mitigation: | Increase budget for high school junior name search, expand high school guidance counselor visits, open admissions office in city in new area, research and present reports on success of recent college graduates in securing gainful employment, develop Return-on-Investment calculation to use in marketing to families of prospective students, increase funding for career center to help place students in internships and jobs upon graduation |

| Likelihood After Treatment: | 2 |
| Impact After Treatment:     | 3 |
| Risk Score After Treatment: | 6 (likelihood x impact); Level 2 |

ERM Step 4. Measure, Track, and Communicate Risks.

Monitoring risks and communicating plans to the campus community are vitally important to a strong ERM program. The risk registers are a starting point and a continuing point of reference; they contain important measuring elements, which can be enhanced with well-placed analytics (e.g., probability and impact). The overall format of a measuring and tracking system varies, and software can help, but the basic idea is most easily conceptualized with a spreadsheet or brief report. For example, a report could follow the format in Figure 2.

Elements of a risk management plan can include the following:

- Risk category (e.g., curriculum, technology, financial)
- Description of the risk
- Responsible officer: Who owns the risk?
- Organizational goal: This is the tie between the risk and the organization’s business goals.
- Likelihood/probability: This can be statistical or simple but should allow the reader to gauge the risk.
- Impact/consequence: What will happen in the worst (or best) case scenario?
- Risk score (impact and likelihood) before and after mitigation
- Mitigation: How can the institution prevent (or guarantee) that scenario?
- Controls in place: On an ongoing basis, how is the risk managed?

Once the risks are measured and tracked, the most important element within step four is communication. This step is not concerned with the volume of information. The quality of the communication is the key, and quality comes through linking a risk with the initiative in an understandable way. Communicating with wide audiences that may not have IT experience is a challenge, but doing so is a critical step in a successful ERM program.

With step four, IT leaders have the opportunity to be a part of, and in some cases lead, the strategic conversation. As previously noted, however, taking advantage of this opportunity to lead is impossible without a firm grasp of the institution and its plans, culture, and language. Although there was a time when IT managers could simply be administrators of technology, that time has passed. Today, having a passion for the institution’s mission is as important as having a passion for technology. The
communication portion of step four is an important way to gain a foothold within the organization as a trusted advisor, and that foothold can lead to greater responsibility and strategic importance for information technology.

Summary
The evolution of information technology—from being a service provider to becoming an integral component of the institution’s mission—has accelerated over the last decade. Technology is critical for research, teaching, and service, the three missions that form the foundation for all colleges and universities. Faculty and administrators are initiating new partnerships and new ventures that can be enhanced (the upside) or destroyed (the downside) as a result of the risks associated with technology and analytics. By leveraging ERM, IT leaders are well positioned to engage with senior administrators and with others throughout the organization.

© 2013 Janice M. Abraham, Robert Baird, and Frank Neugebauer. The text of this article is licensed under the Creative Commons Attribution-NonCommercial-NoDerivs (by-nc-nd) 3.0 Unported License.