Imagine it is not 2013. It is 2008. You are a CIO, and you have just returned from a higher education conference where a panel of IT experts talked about the compliance issues facing the IT department. The compliance issues discussed were not necessarily issues that had a neat IT checklist or that were even predominantly IT issues. But each issue the panel discussed had implications for the IT department, and at your higher education institution, there was not likely anyone else receiving this same information. The issues might rightly have been dubbed information security issues, privacy issues, student services issues, financial aid issues, finance issues, legal issues, or perhaps even policy issues, but the prominent institutional space that was a gathering point for information compliance issues in 2008 was the IT department.
In 2008, being IT compliant was not limited to the discipline of privacy. Privacy, at that time, was a burgeoning specialty, inside or completely independent of the IT department, committed to protecting the value of an individual’s information and answering increased pressure on institutions from new privacy-related laws and data breaches. Privacy was visionary, answering anticipatory concern about the pace of information collection and the dignity of the individual, and it emphasized honor and reputation. Compliance was also not limited to actions performed for information security. Security was processes and technology protecting systems with the aim of confidentiality, integrity, and accessibility of information against a tide of increasingly bold and opportunistic Internet mischief or crime.

In that 2008 higher education conference, the Chief Information Security Officer of one institution and the newly appointed Chief Privacy Officer of another institution (or their equivalents) may have had a spirited debate about the primacy of the precepts governing their given disciplines. Perhaps there was even concurrence. Privacy arguments, especially early on in the debate, centered on the right of individuals to control their private information and the duty of an institution to have processes that protected that privacy. Security proponents argued that no one can have privacy without security—security equalling technology and technology processes. Security, they would have said, is the only way to ensure privacy.

In that 2008 conference, IT compliance was present as the common meeting ground for the differing disciplines. Compliance, in general, looked for specific rules with specific written requirements—no heady philosophies or debates. Whether those requirements were set by law/regulations or by industry standards, or even by an institution’s own policies, the act of compliance was theoretically pushing square pegs into square holes.

At that 2008 conference, one of the speakers would most likely have put up a slide with polysyllabic, hearty, or even acronymic IT compliance issues. In the beginning, said the slide, there was FERPA (Family Educational Rights and Privacy Act). FERPA gained the slide’s first mention because of its age (passed in 1974) and its recognition of “privacy or other right of the students” and because it required a procedure to be in place “for the granting of a request by parents for access to the education records of their children within a reasonable period of time.” FERPA was an introduction to compliance, privacy, and security requirements for higher education. Though the first FERPA legislation was not lengthy, it generated (and continues to generate) significant scholarly treatise and countless hours of education, training, contract clauses, argument, and conjecture. Further compliance issues populating that 2008 slide were representative federal or uniform legal areas that were arguably related to and contained compliance issues affecting the operations of a higher education IT department, such as HIPAA, CALEA, PATRIOT ACT, GLBA, CAN-SPAM, SOX, ECPA, CFAA, DMCA, TEACH ACT, and E-SIGN. All required capital letters because all were acronyms. All also had significant implications for higher education. They were also a judicious preview of how things would change.

In 2013, the same purview of those and other compliance issues is immeasurably more complex because of technology advances. Cloud computing, data analytics, integrated planning and advising systems, identity management, behavior management, cyber-bullying, social networking, nation-state hacking, flash drives, laptops, tablets, smartphones, bit torrent, student outcomes, consumerization, and virtualization, to name a few, have all exploded data into an institutional asset that is expanding in use, proliferation, location, and risk at an unprecedented rate. In 2013, the broad issue of managing data in a legal and compliant manner requires a privacy professional, a security professional, a risk management professional, a policy professional, a data governance professional, a legal professional, and arguably, an ombudsman-like professional versed in every potential issue that may affect the higher education institution and that involves electronic information or communication. In some institutions, all of these roles may be held by one person. In others, a group of professionals from differing departments may be responsible for looking at a regulation or a data set or an activity performed under the auspices of higher education.

In 2013, IT compliance in the exploded technological view necessarily requires privacy and security compliance issues to be fortified with a risk-based approach.
the transition to the higher education institution of 2020.

**IT Compliance Begins with Risk**

I took a risk today: I came into work. I awoke and opened my eyes, gauged my internal temperature, thought about the possibility of sleeping longer, took a run, stepped into the shower, shaved my face, got into my car, negotiated the freeways of Washington, D.C., parked my car, and walked into my building. Several risk calculations had gone into my day's activities, and it was only 8:00 a.m. I turned on my computer. It worked. There was some risk that it would not turn on, that it would turn on and start a fire, or that it would turn on and a message would inform me that some staff member had fallen for a spear-phishing e-mail that had paralyzed the entire college, that some malware had blossomed overnight, that some student had mistaken me for the service desk and asked for a password change . . . the list goes on. For each of us, each day consists of our being affected by our conscious or even unconscious risk management decisions or being the unintended beneficiary of the risk decisions of others.

The etymology of the word *risk* is varied, but one of the most interesting origins comes from the Italian word *ris-care*, which means to “run into danger.” I ran (literally ran) and drove my way into danger today. Running into—or making a decision to avoid—danger is both innate and calculated. Even Neanderthals had to make a determination on whether or not to step into or out of the path of an oncoming herd of wild cattle. Higher education is likewise risky. It is risky to accept a student, to register a student, to house a student, to provide a network, to provide connectivity, to provide a classroom, to provide health-related
services, to teach a student, to grade a student, to receive data, to store data, to conduct research, to hire staff, to pay staff, etc. It is risky to allow hundreds of people at an institution access to personally identifiable information. It is risky to excel. Higher education without risk-taking is yellow pads and #2 pencils. Every brilliant technological innovation present today in higher education was, at one time, risky.

But risk is also a term agnostic of morality. Many risks taken, mitigated, or avoided made perfect arithmetic sense (at the time) yet turned out poorly. Other risks taken, mitigated, or avoided seemed “seat of the pants” whimsical but turned out brilliantly. When we look for how to comply with laws, mandates, policies, and standards, we are invariably, at a baseline, making risk decisions: weighing the good and bad that can result and planning for optimization. Every facet of compliance-centric IT areas—whether policy, security, privacy, or even data governance—requires an assessment of risks and how they will be managed. FERPA, as an example and in its most basic form, requires protection of certain student data against disclosure. No guideline or requirement was originally provided about what that protection might be. To develop procedures, people working in the higher education environment assessed risk about the various methods for complying with this mandate, and they ventured forth.

The Arithmetic of Risk
To understand the risks that we seek to manage down the path of IT compliance, we should further clarify some terms. We all innately understand that risk, along with control of that risk, is a prominent determinant of our success or lack of success in a given endeavor.

Understanding the extent of risk helps institutions look at their strategic and tactical goals, as well as their overall vision. What are the hindrances? What are the roadblocks? Additionally, the arithmetic formulas of risk management are instructive. What does “risk equals threats times vulnerabilities times business impact” (R = T × V × BI) mean? At a basic level, the risk of doing a particular activity might be lessened or eliminated to the extent that there is no threat to that activity or that we are not vulnerable in performing that activity, despite existing threats. Also, if there is no business impact or cost as a result of a vulnerability being exploited by a threat, then risks are lowered or eliminated.

When we look for how to comply with laws, mandates, policies, and standards, we are invariably, at a baseline, making risk decisions.

In the context of securing information, risk is “a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.” Risk will attach to any activity, but an understanding of the nature and depth of the risk helps an institution decide if the risk is one it can live with or can control by acceptance, avoidance, and mitigation.

Threats to that same information are defined as “any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.” Threats can be natural—such as floods, earthquakes, or hurricanes. Threats can be human, through unintentional or intentional actions. Threats can also be environmental. For example, an institution that has a railroad track running through awareness activities, and policies (or lack thereof) used by an institution are also a form of vulnerability. For example, if the population at an institution has not been made aware of the potential damage of phishing e-mails, the vulnerability to being phished increases. If users at another institution have excessive or unchecked access rights, whether to devices or to information, the vulnerability to threats of negligent data breaches increases.

Business impact is defined as “the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.” Sometimes business impact is strictly monetary. If an area at an institution is susceptible to flooding and a flood occurs without any plan to avoid that threat, funds will have to be expended. Or the business impact might be reputational. If an institution breaches donor information often, donors may quit donating.
Let’s look at an example. University A is considering putting all of its employee information (e.g., name, date of birth, address, driver’s license number, social security number, health information, salary information, banking account information, benefit information) onto flash drives in the shape of the university’s mascot so that the Human Resources Department can provide more personalized and face-to-face service. If we assess this proposed mascot-shaped flash drive activity, does the assessment yield risk?

One could argue that there are existing threats. Human error, intentional and malicious actions, and malware are well-known threats. People could lose or misplace the flash drive. The flash drive could be stolen.

If we then look for vulnerabilities for these threats to exploit, which do we see? One vulnerability might be that these flash drives are (possibly) unencrypted, so if one is stolen or lost, all the information could be intentionally or unintentionally breached. Another fairly obvious vulnerability is that the user rights granted to the data on these flash drives might be viewed as excessive.

Finally, what about business impact? A picture on the front page of University A’s local newspaper of a flash drive in the shape of a cuddly mascot detailing the loss of information to students, staff, or donors would likely have substantial financial, regulatory, legal, and reputational impact. Thus the proposed activity contains arguably substantial organizational risk.

Risk Assessment, Risk Treatment, and Collaboration

The risk assessment of a proposed activity yields specific or non-specific risk, and an organization must then determine how this risk can be treated. Risk treatment activities may occur formally in a checklist or informally within settings that may never actually mention the word risk. Risk treatment generally flows into the following courses of action:

- Knowingly and purposefully accepting risks, provided the risks meet the organization’s policy and criteria for risk acceptance
- Applying appropriate controls to reduce the risks
- Avoiding risks by not allowing actions that would cause the risks to occur
- Transferring the associated risks to other parties, e.g., insurers or suppliers?

All of the above-mentioned risk treatment options necessarily involve collaboration. If an HR department were to propose the mascot-shaped flash drives for use inside the institution’s walls, does that institution have the wherewithal to collaboratively determine risk treatment? Was the institution’s information security function—or the compliance function, or the privacy function, or the risk management function, or the data governance function, or the policy function, or the legal function—consulted? A proposed risk-impacted activity viewed within the silo of only one part of an institution will yield a partial view of the risk or the potential treatment of that risk. One can imagine the regular meeting of that institution’s compliance (or equivalent) function at which the activity involving flash drives is first discussed. After a brief moment of silence, stunned or contemplative, the discussion of risk and risk treatment could commence.

Controls as Risk Treatment

The application of controls at the outset of a proposed activity can influence the risk at various parts of the process. Preventive controls, as the name implies, act to prevent the acknowledged threats from exploiting vulnerabilities. In information security, control activities that can block or reduce a threat’s impact include proper authentication, access control enforcement, firewalls, routers, VPN, desktop security, and intrusion detection.

Detective controls are set to operate during an exploit incident to characterize the nature of the incident; they can sound the alarm. In information security, self-assessment and vulnerability scans can act to identify and reduce vulnerabilities, while intrusion prevention and network monitoring are examples of controls that operate during an exploit to reduce impact.

Administrative controls are also used to reduce vulnerabilities that can be exploited. These are controls aimed

The risk assessment of a proposed activity yields specific or non-specific risk, and an organization must then determine how this risk can be treated.
exist as a result of unacceptable uses and the impact that vulnerability can have. Institutional policies concerning myriad topics such as data classification, data stewardship, data security, least privilege policies, and policies limiting the use of certain personally identifiable information, along with education and awareness efforts, can reduce vulnerability to an institution.

Controls can be physical as well as technical. Fire extinguishers, fences, guards, gates, lights, and locked doors are all examples of physical controls that may be used to reduce exploits, vulnerabilities, or impact. Together, the technical, administrative, and physical controls form the bulk of a treatment plan after risk has been assessed.

**IT Compliance Meets Risk Assessment**

**Meets Risk Control Requirements: GLBA**

Back in the 2008 conference on compliance issues, the Gramm-Leach-Bliley Act (GLBA) would have been mentioned with prominence. It still applies today. The GLBA is a federal law that was enacted by Congress in 1999. The opening section of the law, Section 6801, explains its purpose: “It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers’ nonpublic personal information.” Institutions of higher education were included in the reach of GLBA because in the process of daily financial aid operations, higher education collects and maintains financial information on students and others. Though this is a narrow data subset for any higher education institution, it is a powerfully impactful subset.

The Federal Trade Commission (FTC) promulgated rules to implement the GLBA. The FTC first implemented the “GLBA Privacy Rule” in 2000. The GLBA Privacy Rule, while disagreeing with those “who suggested that colleges and universities are not financial institutions,” also acknowledged that colleges and universities “are subject to the stringent privacy provisions in the Federal Educational Rights and Privacy Act (‘FERPA’), 20 U.S.C. 1232g, and its implementing regulations, 34 CFR part 99, which govern the privacy of educational records, including student financial aid records.”

Any institution, therefore, that was FERPA-compliant for privacy purposes was also compliant for GLBA purposes.

The FTC also created the GLBA Safeguards Rule in 2002, effective May 23, 2003. Institutions of higher education were not exempt by virtue of other compliance activities. The Safeguards Rule introduction was straight out of risk management parlance: “As required by section 501(b), the standards are intended to: Ensure the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer.” The rule requires a comprehensive written information security program as part of an institution’s GLBA compliance efforts. Further requirements include designating an employee to coordinate the information security program, identifying risks to the “security, confidentiality, and integrity” of consumer data, and establishing a program of controls that “design and implement information safeguards to control the risks [identified] through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards’ key controls, systems, and procedures.”

Compliance with GLBA (and with other laws such as HIPAA) requires an institution to mesh privacy, security, risk management, data governance, and policy into one effort; embarking on that effort requires the collaboration of several individuals or departments within an institution. GLBA introduces risk controls that were already a part of the architecture at most institutions, and it harmonizes those controls as part of the fabric of IT compliance. With an understanding that compliance involves not only federal and state laws but also institutional policies and standards, a risk-based approach to compliance can yield better internal institutional understanding and buy-in.

**Extending IT Compliance Efforts to Privacy and Security**

Different standards provide controls to manage risk, based on the discipline. Standards organizations such as the International Organization for Standardization (ISO), the National Institute of Standards and Technology (NIST), the IT Infrastructure Library (ITIL), and the Information Systems Audit and Control Association (ISACA) all provide a broad range of standards for industry, the federal government, and/or higher education.

practices including the selection, implementation and management of controls taking into consideration the organization’s information security risk environment(s). ISO 27002:2013 contains 14 sections, with 35 control objectives and over 100 controls, including policy, organization of information security, human resource security, asset management, physical and environmental control, and others. The higher education “Information Security Guide,” written by IT professionals from representative institutions of higher education, is based on the ISO/IEC 27002 model.

Privacy risk management relies on the same assessment methodology as information security risk management and has evolved from a guideline approach to specific privacy control mechanisms. In 1980, the Organization for Economic Cooperation and Development (OECD) adopted the “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.” The Guidelines anticipated that unanimity would be required to keep private information flowing intentionally across borders, especially as the information economy grew. “The drafters of the Guidelines foresaw that technology would develop rapidly, and the principles set forth in the Guidelines were designed in a technology-neutral way to accommodate future developments.” When examined in light of a pre-Internet era, the OECD Guidelines are prescient. They specify principles on limiting the collection of information, on the quality of the personal data collected, on the purposes of data collection, on limiting the use of data, on security safeguards to be put into place, on participation by the individual whose information is collected, and on accountability by the gatherer of information. Under the OECD Guidelines, information security is on par with any other principle. The Security Safeguards Principle states: “Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.”

The Generally Accepted Privacy Principles (GAPP), introduced by the American Institute of CPAs and the Canadian Institute of Chartered Accountants in 2003 and last updated in 2009, include principles on management, notice, choice and consent, collection, use and retention, access, disclosure to third parties, security for privacy, quality, monitoring, and enforcement. The security requirements have developed into substantial controls in the latest draft, including the requirements of policy, notice, risk assessment, and security controls.

In 2013, NIST finalized a document for privacy controls in its update to Special Publication 800-53: “Security and Privacy Controls for Federal Information Systems and Organizations.” The document considered privacy controls as part of the same document that requires security controls: “Privacy, with respect to personally identifiable information (PII), is a core value that can be obtained only with appropriate legislation, policies, procedures, and associated controls to ensure compliance with requirements.” The document embraces privacy and risk assessments, data minimization, privacy awareness and training, data retention, test data, and notice, among others, as privacy controls.

Consumerization, Reputational Risk, and Opportunities
As I completed my fantasy football draft on my spouse’s iPad the other evening, I silently took count of our “consumer” devices. We have two laptops, two smartphones, and two iPads. This count did not include devices provided by my or my spouse’s institution. Each one of our devices contains applications or programs that we have added because we felt they functionally improved our daily lives or because peers had told us the applications were pretty cool.

In the institutional environment, students, faculty, and staff increasingly arrive with their own devices and also use institutionally provided devices and services each day. Barring restrictive
BYOD (Bring Your Own Device) security, those devices are populated with inexpensive user-friendly consumer applications and programs that users believe functionally improve their studies, their work space, their efficiency, their quality of life, and/or their eye-hand coordination (ergo, “consumerization”). Those same devices may contain institutional data or even personally identifiable information. In a report issued in early 2013, the EDUCAUSE Center for Applied Research (ECAR) found the proliferation of devices to be “manic”: “Device proliferation is manic, and unmanaged growth could result in a ‘tragedy of the commons’ situation, where too many devices find their way to campus networks too fast and institutions find more opportunities lost than taken.” The ECAR report represents the discussion of risk at its best: device proliferation is presenting us with a risky time in higher education, and proper attention to risk control decisions, such as securing data, managing access, securing systems and networks, and managing identity and authentication, along with raising user awareness, can elevate and leverage technology and thus the institution’s reputation positively. The obverse also is true. If these risks (opportunities) are poorly managed, the institution’s reputation could be impacted negatively.

Reputational risk decisions weave their way through every facet of the IT organization and every other department within an institution and influence compliance decisions. When personal computers were first deployed, there were no networks, and each user managed his or her personal system. Users controlled what software they had and the updates to that software, and they called the IT organization when things went awry. With the proliferation of
The intricacies of privacy, information security, data governance, and IT policy as compliance and risk areas within the IT organization can reverberate and impact every other department within the higher education institution.

networks and centralized workstation management (positive controls) and the impact of hacking, data leakage, and breaches (new threats), institutions have had the momentum if not the clear guidance to tighten up risk control areas such as access controls (whether to devices or data), privacy processes, encryption of devices, authentication, data proliferation/minimization, credit card usage, and least privilege concepts. Now with networked devices per student increasing rapidly and the accompanying strain on resources becoming a top IT issue, reputational risk is at stake both positively (bring any device and use it how you want) and negatively (but do not let a breach, phishing, hacking, or malware incident occur). The risk assessment of any proposed technology-centric activity has to have broad vision, be collaborative, and not be limited to technology.

Conclusion
In 2013, compliance issues march, unceasingly, through every aspect of higher education. Yet the intricacies of privacy, information security, data governance, and IT policy as compliance and risk areas within the IT organization can reverberate and impact every other department within the higher education institution. The primary focus is always the information that is received, managed, shared, stored, or destroyed as part of the daily procedures inside any institution.

IT compliance in 2013 is blended inside multiple institution functions. Managing risk as an integral part of compliance is an attempt to lower the odds that a bad event will occur or to increase the odds that a good event will occur. Some element of risk will always exist. Incidents, data breaches, hacking, falling for phishing e-mails, viruses, and malware will still affect operations in higher education, though hopefully with lower frequency and severity. Controlling the impact of risks after a vulnerability has been exploited will remain as important as preparing for risks in advance. Only through collaborative compliance and risk discussions can appropriate decisions be made about both the everyday activities and the transformative new technologies that are or will be available to the higher education institution of 2020.

Notes
1. United Nations, General Assembly, 3rd Session, Resolution 217A Universal Declaration of Human Rights, 1948. The International Covenant on Civil and Political Rights was adopted by the General Assembly of the United Nations in Resolution 2200A (XXI), December 16, 1966. For the full text of the Resolution and the Covenant, see Official Records of the General Assembly, 21st Session, Supplement No. 16 (A/6316), p. 49. (“No one shall be subjected to arbitrary interference with his Privacy, family, home or correspondence, nor to attacks on his honour or reputation.”)
4. Ibid., p. 8.
5. Ibid., p. 9.
6. Ibid., p. 11.
12. Ibid. Summary of controls found at https://www

© 2013 Patrick J. Feehan. The text of this article is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike (by-nc-sa) 3.0 Unported License.

Patrick J. Feehan (patrick.feehan@montgomerycollege.edu) is Director, IT Privacy and Cybersecurity Compliance, at Montgomery College.