Understanding and Managing the Risks of Analytics in Higher Education: A Guide

June 2012

Randall J. Stiles
About the Author

Randy Stiles is special advisor for the president at Colorado College. He supports the president in strategic thinking, planning, and new initiatives, giving special emphasis to enhancing the college’s business intelligence capabilities. He served as the college’s vice president for information management between 2003 and 2011, overseeing the offices of institutional research and planning as well as IT services.
# Table of Contents

Executive Summary ................................................................................................................. 5  
Introduction ............................................................................................................................. 9  
Decision Making in Higher Education .................................................................................... 11  
Risk Management and the GRC Framework ........................................................................... 12  
Understanding and Managing the Risks of Analytics ............................................................ 14  
  Risks for Institutional Leaders .............................................................................................. 15  
    Inappropriate or Premature Use of Analytics ....................................................................... 15  
    Countercultural Implementation of Analytics ...................................................................... 17  
    The Risk of Saying “No” or “Not Now” to Analytics ......................................................... 19  
Data and Information Governance Risk .................................................................................. 20  
Data and Information Quality Risk .......................................................................................... 25  
Data and Information Compliance Risk .................................................................................. 28  
Special Topics in Risk Management ....................................................................................... 30  
  Institutional Use of Data for Learning Analytics ................................................................. 30  
  Third Parties—Cloud and Software-as-a-Service Issues  
    (includes sample contract terms and conditions) .............................................................. 33  
Conclusion .............................................................................................................................. 36  
Appendix .................................................................................................................................. 39  
  Additional Risk Management Considerations ....................................................................... 39  
  Degrees (or Layers) of Protection .......................................................................................... 41  
  Data Protection Technologies ............................................................................................... 42  
Acknowledgments .................................................................................................................... 44  
Recommended Readings ........................................................................................................... 44
Illustrations

Figures

Figure 1. A roadmap for this guide ................................................................. 10
Figure 2. Risk management principles and process ...................................... 13
Figure 3. The governance, risk management, and compliance framework .... 14
Figure 4. The learning analytics concept .................................................... 31
Figure 5. Key considerations in third-party service contracts .................... 34
Figure 6. Organizing for effective analytics practice in higher education .... 37

Tables

Table 1. Data governance checklist ............................................................... 20
Table 2: Data sensitivity classification .......................................................... 24
Table 3. Dimensions of data quality ............................................................ 26
Table A.1. Data value classification and quantification ................................. 40
Table A.2. Degrees of protection ................................................................. 41
Table A.3. Data protection technologies .................................................... 42
Executive Summary

In Why Does College Cost So Much? and The Innovative University: Changing the DNA of Higher Education from the Inside Out, the authors describe some key factors affecting decision making in higher education today. Due to increases in the value of higher education to economic competitiveness and upward mobility, sustained increases in the cost of higher education, growing scrutiny and demands for accountability (by accrediting agencies and the government), and the transformative “disruptive innovation” forces of online learning and outcomes-based assessment, higher education decision makers are exploring the relatively new waters of analytics. Within EDUCAUSE, the working definition of this term is “the use of data, statistical analysis, and explanatory and predictive models to gain insights and act on complex issues.” Making better, data-informed decisions, improving performance, and becoming less reliant on “gut instinct” regarding critical issues facing the institution or the quality of instruction are all worthy pursuits. However, a decision to invest institutional resources in analytics is not without risk, so a fair-minded analytical thinker should consider the risks and how to manage them. Because of the close connections between the practice of risk management and matters of governance and compliance, it is increasingly common to do this work within a governance, risk management, and compliance (GRC) framework.

In Analytics at Work: Better Decisions, Better Results, Thomas Davenport and his co-authors make the case for analytics with the following cautions:

- In some instances the use of analytics doesn’t apply.
- Sometimes the use of analytics is not practical.
- Occasionally decisions informed by analytics need scrutiny.
- Ultimately, even when analytics does apply, the best decisions will be made by those who “combine the science of quantitative analysis with the art of sound reasoning.”

With those broad cautions in mind, this guide highlights five specific risk areas to address in an analytics initiative:

- Risks for institutional leaders
- Data and information governance risk
- Data and information quality risk
- Data and information compliance risk
• Special risks, specifically, those associated with “learning analytics” and the use of cloud services or software as a service (SaaS)

Additional risk management considerations are addressed in the appendix.

**Risks for Institutional Leaders**

**Inappropriate or Premature Use of Analytics Risk.** There are situations when the tools and methods of analytics aren’t practical and cases where decisions informed by analytics need scrutiny. For example, analytics likely will not be helpful for decision makers when there is no time for gathering, processing, and interpreting data; when there is no history or precedent related to the decision or when historical data may be misleading; when the decision makers have legitimate expert experience and intuition; and when key variables can’t be measured or have very high degrees of uncertainty.³

A second caution concerns the difficulty of the measurement. For example, the assessment of student learning outcomes has been the subject of a great deal of study and debate since the mid-1980s; measuring the quality of learning and teaching is important but quite complex.⁴ Research productivity has more quantifiable metrics. Just because something can be measured easily doesn’t mean that it is more important or should get more attention than something that is difficult to measure.

Finally, an institution may not be ready for effective analytics work. In a *Harvard Business Review* article, Shah et al. describe four problems that prevent organizations from realizing better returns on their investments in analytics:

• Analytics skills are concentrated in too few employees
• IT needs to spend more time on “I” (information) and less on the “T” (technology)
• Reliable information exists but is hard to locate
• Business executives don’t manage information as well as they manage talent, capital, and brand⁵

**The Risk of Countercultural Implementation of Analytics.** A study of analytics work by the Sloan Management School and IBM highlighted the importance of a *data-oriented culture*, i.e., a pattern of behaviors and practices by a group of people who share a belief that having, understanding, and using certain kinds of data and information plays a critical role in the success of their organization.⁶ Imposing analytics initiatives in an organizational culture that is not data-oriented can pose a significant risk to leaders, ranging from ineffectual implementations that have minimal value for organizational decision making to outright failures leading to fundamentally misinformed, inaccurate decisions. Shah et al. provide additional insights regarding this issue. They surveyed and evaluated 5,000 employees in 22 global companies based on their decision-making style: *unquestioning empiricists* trust analysis
over judgment, *visceral decision makers* rely exclusively in intuition, and *informed skeptics* “effectively balance judgment and analysis, possess strong analytics skills, and listen to others’ opinions but are willing to dissent.” They found that the functions performed by those in the informed-skeptics category were at a higher level than for those in the other two, but that just 38% of employees and 50% of senior managers fell into this category. The implication for higher education leaders is that plans for analytics initiatives should include an assessment of the organizational decision-making style and the degree to which organizational culture is data-oriented.

**The Risk of Saying “No” or “Not Now” to Analytics.** Champions of analytics promise better decisions and better results. And, there is evidence within the business world that those companies that have developed a data-friendly culture and have made analytics investments are gaining a strategic advantage over their competitors. In higher education, some institutions are beginning to report success with learning analytics initiatives, leading to significant improvements in retention and learning outcomes. Examples include the work at Rio Salado Community College and the Purdue University Signals Program. If the local culture favors decisions based on intuition rather than analytics, the risks of pushing too hard and too soon on analytics may outweigh those of decisions based exclusively on intuition. However, the potential inability to respond effectively to a challenging policy environment at the board, state, or federal level; the potential inability to demonstrate institutional efficiency and effectiveness; and/or the potential damaging effects of strategic planning decisions based on “gut instinct” may pose significant risks.

**Data and Information Governance Risk**
To ensure data and information privacy, security, quality, and auditability, they must be carefully controlled, which is a governance issue. Data and information governance risk can be mitigated with carefully conceived and well-written policy documents. It is through the utilization of risk management principles and processes that appropriate levels of control can be realized. The data governance checklist associated with Family Educational Rights and Privacy Act (FERPA), the risk analysis elements from the Health Insurance Portability and Accountability Act (HIPAA) guidance, and the EDUCAUSE resources highlighted in this guide all serve as helpful resources for policy development and risk management.

**Data and Information Quality Risk**
“You can’t be analytical without data, and you can’t be really good at analytics without really good data.” Decision makers need data and information (meaningful patterns of data) that communicate and promote understanding of complex issues. Stephen Few and Edward Tufte offer helpful ideas about the art and science of data visualization, including how to identify patterns and make meaning from data. Data and information quality risk can be mitigated by
identifying data stewards and giving them responsibility for developing an inventory of institutional data and information, ensuring there are clear definitions and quality standards for all data and information, and establishing and exercising a data and information quality review and improvement process, targeting those data and information elements that matter most.

Data and Information Compliance Risk
Compliance means conforming to the requirements of an authorized and recognized external agent—usually associated with a law (state, federal, or international) or contract—as well as the enforcement of internal policies. Failure to comply can lead to an adverse result such as a financial penalty, additional work, or even personal liability and imprisonment for institutional officers, thus the connection to risk. While the data and information privacy and security compliance requirements of federal laws such as FERPA, the Gramm-Leach-Bliley Act (GLB), and HIPAA are complex and sometimes confusing, investing in compliance work will likely reduce the risks of analytics because such investments will increase data and information awareness, quality, and protection. Those in college and university governance roles must decide how to allocate resources for compliance to achieve an acceptable level of risk.

Special Topics in Risk Management
The increasing use of cloud services and SaaS in higher education is resulting in new governance challenges. It is important to note that ultimately the data-owning organization cannot abrogate responsibility for data protection. Also, the data and information envisioned for use in learning analytics presents new ethical issues for faculty and staff. EDUCAUSE provides an increasing store of resources that can be helpful for such issues.11

Concluding Thoughts
This guide provides an introduction to the major risk categories faced by a higher education institution considering investments in time, energy, and money in analytics work. Under the right circumstances, decision making can be enhanced by the tools and techniques of analytics; large data sets, analytics engines, and new data visualization techniques have considerable potential to enhance both student learning and institutional business intelligence. However, careful consideration must be given to the risks of such investments for those in institutional leadership roles as well as the risks associated with data and information governance, compliance, and quality.
Introduction

In higher education, our common purpose is to provide students with programs and experiences that help them think and learn. The faculty, administrators, and staff doing this work operate in an increasingly complex and competitive environment. And as the costs of higher education have risen, so have the calls for increased accountability. While being analytical has long been highly valued in college and university contexts as a key element of critical thought, using modern analytics tools and techniques constitutes a relatively new approach to support decision making for both administrators and faculty.

Suppose that a new university chancellor or college president joins your institution with a mandate to implement an effective analytics program, or to significantly enhance ongoing analytics work. Making data-informed and better decisions, improving performance, and becoming less reliant on “gut instinct” regarding critical issues facing the institution or the quality of instruction are all worthy pursuits. But given such a mandate, a fair-minded and analytical leader can and should consider the risks as well as the merits of the work that lies ahead.

The purpose of this guide is to address the risks of implementing analytics initiatives, functions, and services at a higher education institution. It provides frameworks, suggestions, and resources that may prove helpful in considering risk and performing analytics at both ends of a possible spectrum—not doing enough or doing too much, too soon. The guide begins by providing background on the motivation and context for using analytics in higher education decision making and the basic concepts and principles of risk management (figure 1). Following this introduction, the guide includes a discussion of, recommended resources for addressing, and mitigation strategies regarding the risks of:

- Inappropriate, premature, or countercultural uses of analytics, as well as the risks of saying “no” or “not now” to analytics
- Failure to establish proper governance policies and processes
- Poor data and information quality
- Failure to meet compliance requirements for data and information

Data protection, including matters of privacy, security, governance, and compliance, is a key risk that must be addressed because of the fundamental importance and use of data and information in analytics work. Therefore, the guide also includes a discussion of several special topics with suggestions regarding:

- Institutional use of data for analytics, such as how FERPA might impact the use of student academic records in learning analytics efforts
• Access and use of institutional data by third-party systems and service providers, such as when an institution entrusts its data warehouse development, management, and “business intelligence” reporting to a cloud services company
• Sample terms and conditions colleges and universities might incorporate into contracts with relevant systems and service providers to ensure privacy and security risks are appropriately addressed

The appendix provides additional risk management considerations beyond the principles and processes contained in the guide to further assist institutions in addressing the broad array of analytics-related issues they may encounter.

Figure 1. A roadmap for this guide
Decision Making in Higher Education

…education is a critical component of the American dream of rising living standards from one generation to the next, and of social mobility as a result of hard work and achievement. Public opinion surveys consistently find that how much one has to pay for a college education is a serious national concern. (Robert B. Archibald and David H. Feldman, Why Does College Cost So Much? [New York: Oxford University Press, 2011], 7)

For the first time since the introduction of the printed textbook, there is a new, much less expensive technology for educating students; online learning. Simultaneously, more outcome-oriented accreditation standards have begun to level the competitive playing field; it is no longer as important to evidence educational capacity via brick-and-mortar facilities and Ph.D.-trained faculty as to demonstrate student learning. (Clayton M. Christensen and Henry J. Erying, The Innovative University: Changing the DNA of Higher Education from the Inside Out [San Francisco: Jossey-Bass, 2011], xxiii-xxiv)

These quotes capture some key factors affecting higher education decision making. As a result of increases in the value of higher education to economic competitiveness and upward mobility, sustained increases in the cost of higher education, growing scrutiny and accountability (by accrediting agencies and the government), and the transformative “disruptive innovation” forces of online learning and outcomes-based assessment, higher education decision makers are exploring the relatively new waters of analytics. Within EDUCAUSE, the working definition of analytics is “the use of data, statistical analysis, and explanatory and predictive models to gain insights and act on complex issues.” Much more about analytics concepts in higher education and the still-developing terminology can be found in recommended readings 1 through 8.

Recent research in the social sciences and neuroscience is revealing more about the complexity of human decision making (see recommended readings 9 and 10, for example). Higher education leaders at all levels regularly confront cost/benefit-type decisions as well as those related to morality and cultural norms. Colleges and universities have reputations for slow and deliberate change, with an important role for faculty governance, which may be beneficial in some respects. Kahneman notes the power of organizational decision-making processes as follows:

Organizations are better than individuals when it comes to avoiding errors, because they naturally think more slowly and have the power to impose orderly procedures. Organizations can institute and enforce the application of useful checklists, as well as more elaborate exercises such as reference-class forecasting and premortem. At least in part by providing a distinctive vocabulary,
organizations can also encourage a culture in which people look out for one another as they approach minefields. Whatever else it produces, an organization is a factory that manufactures judgments and decisions.¹²

A second way to improve human decision making (at all levels) is through the use of analytics. The argument for analytics is that with large data sets, powerful analytics engines, and skillfully designed visualization techniques, we can use the experience of the past to create helpful models of our processes; we can even more effectively use real-time data and information to alert us to matters requiring our attention; and we can (in some cases) extrapolate to the future using predictive modeling and optimization techniques. A 2011 study sponsored by IBM and MIT’s Sloan School of Management found a widening performance gap between “transformed” businesses (those that had successfully employed analytics techniques) and those that were still in an aspirational stage with such techniques.¹³ And in an EDUCAUSE Review article, Phil Long and George Siemens suggest that “learning analytics” may soon allow faculty and students to “penetrate the fog” surrounding teaching and learning—practices that have long been guided by heuristics.¹⁴ While the results of such initiatives are just beginning to surface, it is clear that analytics in higher education is gaining attention.

**Risk Management and the GRC Framework**

In *Against the Gods: The Remarkable Story of Risk* (recommended reading 11), Peter Bernstein provides a thorough and enjoyable description of the evolution of thought that has led to the contemporary understanding and use of risk management concepts.¹⁵ He argues that the idea of risk management is so important that it differentiates ancient and modern times: it suggests that man, not the gods, might gain control over the future.

> The ability to define what may happen in the future and to choose among alternatives lies at the heart of contemporary societies. Risk management guides us over a vast range of decision-making, from allocating wealth to safeguarding public health, from waging war to planning a family, from paying insurance premiums to wearing a seatbelt, from planting corn to marketing cornflakes.

Methods of risk management, regardless of the area of application, usually involve the identification and description of threats, an assessment of the risk associated with those threats and vulnerabilities (probability of occurrence and associated consequences), the identification of ways to avoid or mitigate the threats and vulnerabilities, a prioritization of risk-reduction measures, and resource allocation decisions corresponding to the priorities. Risk management is an example of analytics at work. Figure 2 provides a high-level summary of risk management principles and process from ISO, the International Organization for Standardization.¹⁶ Later in this guide, more details regarding risk management techniques for data protection will be reviewed in the context of governance and compliance.
Due to the important relationship between the three concepts of governance, risk management, and compliance in any organization, an emerging trend in business and higher education is the use of the GRC framework. This relationship, illustrated in figure 3, can be understood by adding definitions of **governance** and **compliance** to the risk management principles and processes noted above:

**Governance** describes the overall management approach through which senior executives direct and control the entire organization, using a combination of management information and hierarchical management control structures.

**Compliance** means conforming with stated requirements. At an organizational level, it is achieved through management processes which identify the applicable requirements (defined for example in laws, regulations, contracts, strategies and policies), assess the state of compliance, assess the risks and potential costs of non-compliance against the projected expenses to achieve compliance, and hence prioritize, find and initiate any corrective action.17

---

### Risk Management Principles and Process

<table>
<thead>
<tr>
<th><strong>Principles</strong></th>
<th><strong>Process</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>- Create value – resources expended to mitigate risk &lt; consequence of inaction</td>
<td>- What’s the scope?</td>
</tr>
<tr>
<td>- Should be an integral part of organizational processes and decision-making</td>
<td>- What data and information are available?</td>
</tr>
<tr>
<td>- Systematic and structured</td>
<td>- What are the threats and vulnerabilities?</td>
</tr>
<tr>
<td>- Based on best-available information</td>
<td>- What are current measures to mitigate risk?</td>
</tr>
<tr>
<td>- Tailorable</td>
<td>- What is the probability of the threat occurrence?</td>
</tr>
<tr>
<td>- Account for human factors</td>
<td>- What is the level of risk for each occurrence?</td>
</tr>
<tr>
<td>- Transparent and inclusive</td>
<td>- What is the resultant risk index?</td>
</tr>
<tr>
<td>- Dynamic, iterative, and responsive to change</td>
<td>- What are the options for risk mitigation?</td>
</tr>
<tr>
<td>- Capable of continuous improvement</td>
<td>- What are recommended actions and associated decisions?</td>
</tr>
<tr>
<td>- Periodically reassessed</td>
<td></td>
</tr>
</tbody>
</table>

Source: International Organization for Standardization

Figure 2. Risk management principles and process
Because higher education is deeply rooted in faculty governance, a top-down approach to governance may be problematic. However, federal laws such as FERPA, GLB, and HIPAA make education and implementation through the compliance leg advisable. While a GRC program may be conceived and implemented for the entire college or university, a common segmentation is into the financial, IT, legal, and other administrative areas.

Beyond the basic principles and processes of risk management, one must have a deep understanding of data and information management (e.g., architecture, transformation, movement, storage technologies, integration, etc.) if risks are to be assessed. David Hill’s book *Data Protection: Governance, Risk Management, and Compliance* (recommended reading 12) is an excellent resource in this regard. The appendix includes guidance and tables from this book.

**Understanding and Managing the Risks of Analytics**

In the introduction to *Analytics at Work: Smarter Decisions, Better Results*, Thomas Davenport and his co-authors make the case for analytics with the following cautions:

- In some instances the use of analytics doesn’t apply.
- Sometimes the use of analytics is not practical.
- Occasionally decisions informed by analytics need scrutiny.
- Ultimately, even when analytics does apply, the best decisions will be made by those who “combine the science of quantitative analysis with the art of sound reasoning.”

With those broad cautions in mind, this guide highlights five specific risk areas to address in an analytics initiative:
• Risks for institutional leaders
• Data and information governance risk
• Data and information quality risk
• Data and information compliance risk
• Special risks, specifically, those associated with “learning analytics” and the use of cloud services or software as a service (SaaS)

While the first area will likely be of greatest interest to senior leaders, the others pertain to those at all levels of the institution who might be involved in analytics work.

Risks for Institutional Leaders

Inappropriate or Premature Use of Analytics
In Analytics at Work, Davenport et al. describe situations when tools and methods of analytics are not practical and cases where decisions informed by analytics need scrutiny. Analytics likely won’t be helpful for decision makers when there’s no time for gathering, processing, and interpreting data; when there isn’t a history or precedent related to the decision or when historical data may be misleading; when the decision makers have legitimate expert experience and intuition; and when key variables can’t be measured or have very high degrees of uncertainty. The authors also provide the following list of typical decision-making errors.

Logic Errors
• Not asking the right questions
• Making incorrect assumptions and failing to test them
• Using analytics to justify what you want to do (gaming or rigging the model/data) instead of letting the facts guide you to the right answer
• Failing to take the time to understand all the alternatives or interpret data correctly

Process Errors
• Making careless mistakes (transposed numbers in a spreadsheet or a mistake in a model)
• Failing to consider analysis and insights in decisions
• Failing to consider alternatives seriously
• Using incorrect or insufficient decision-making criteria
• Gathering data or completing analysis too late to be of any use
• Postponing decisions because you’re always dissatisfied with the data and analysis you already have

A second caution concerns the difficulty of the measurement. For example, the assessment of student learning outcomes has been the subject of a great deal of study and debate since the mid-1980s; measuring the quality of learning and teaching is important but quite complex.
Research productivity has more quantifiable metrics. Just because something can be measured easily doesn’t mean that it is more important or should get more attention than something that is difficult to measure. Some researchers in higher education analytics make a distinction between “academic analytics” and “learning analytics.” The first is closely related to business intelligence and the administrative functions (especially finance, legal, IT, and other administrative areas) of colleges and universities. The second is more akin to the assessment of student academic achievement and actions taken in response to that assessment. In either case, effective analytics initiatives need to target metrics that matter most to the institution and in ways that account for the complexity of the measurement. Clayton Christensen and Henry Erying provide useful insights about meaningful measures of success:

Only recently have government regulators demanded accountability for the educational benefits universities produce and the efficiency with which they produce them: What does college cost? How many students are admitted? How many graduate? How long does it take them to graduate? How many get good jobs? At the same time, accrediting bodies have changed their measurement emphasis from inputs and activities to outcomes.\(^\text{21}\)

They suggest a list of “additional success measures” (beyond traditional measures and more outcomes-focused at the institutional level) for students, subjects, and scholarship that include quality dimensions, e.g., the quality of the general education program and the quality of the majors. These are examples of significant metrics that are important but difficult to assess.

Finally, leaders at all levels need to be aware of key barriers to the effective use of analytics. In a *Harvard Business Review* article, Shah et al. discuss how they surveyed and evaluated 5,000 employees in 22 global companies based on their decision-making style: *unquestioning empiricists* trust analysis over judgment, *visceral decision makers* rely exclusively in intuition, and *informed skeptics* “effectively balance judgment and analysis, possess strong analytics skills, and listen to others’ opinions but are willing to dissent.”\(^\text{22}\) They found that the functions performed by those in the informed-skeptics category were at a higher level than those in the other two, but that just 38% of employees and 50% of senior managers fell into this category. They also describe four problems that prevent organizations from realizing better returns on their investments in analytics:

- Analytics skills are concentrated in too few employees.
- IT needs to spend more time on the “I” (information) and less on the “T” (technology).
- Reliable information exists but is hard to locate.
- Business executives don’t manage information as well as they manage talent, capital, and brand.
To mitigate the risk of inappropriate or premature use of analytics, be wary of situations where the tools and methods of analytics are not practical and where decisions informed by analytics require scrutiny. Just because something can be measured easily doesn’t mean that it’s more important or should get more attention than something that’s difficult to measure. Is there necessary and sufficient analytical talent on campus to make effective use of analytics? Is it being managed well? Are the people in these roles “informed skeptics”? Is there a strong relationship between the IT and institutional research functions on campus? If the answer to these questions is “no,” finding strategies to remove these barriers might prove helpful.

Countercultural Implementation of Analytics

The business world has embraced analytics practices. In a 2011 Bloomberg Businessweek study regarding the then-current state of business analytics, 97% of 930 respondents to a global survey indicated that they use some form of analytics in their work. However, one of the findings in this and other surveys of business communities is the importance of a data-oriented culture. For example:

Data-oriented culture: a pattern of behaviors and practices by a group of people who share a belief that having, understanding and using certain kinds of data and information plays a critical role in the success of their organization. In a data-oriented culture, behaviors, practices and beliefs are consistent with the principle that business decisions at every level are based on analysis of data. Leaders within organizations that have mastered this competency set an expectation that decisions must be arrived at analytically, and explain how analytics is needed to achieve their long-term vision.

The authors of that study provide the following advice regarding the development of an analytical culture:

- **Stay the course**—the shift to analytics is a long-term endeavor.
- **Get the executives on board**—effective users of business analytics (86%) are nearly always in organizations where executive management places a great deal of trust in the results of analytics.
- **Data comes first**—before embarking on analytics initiatives, organizations need to assess the effectiveness of their data-management strategies.
- **Move into new analytics technology boldly**—e.g., model management, optimization, and web analytics.
- **Share the knowledge**—in developing the analytics culture, “silo-busting” is essential.
- **Integrate**—beyond collaboration, integration of analytics work across the entire organization is key to success.
• **Hire the right talent**—in developing a functional analytics culture, the linchpins are people.

• **Find your equilibrium**—the average mix of intuition to analytics in decision making is 60/40; each organization needs to find its point of equilibrium in this regard.

Davenport and his co-authors devote an entire chapter of their book to strategies for building an analytical culture. Also, throughout the book they make reference to a five-stage organizational developmental model they call the “DELTA” transitions: for each of the five stages (analytically impaired, localized analytics, analytical aspirations, analytical companies, and analytical competitor), they describe organizational attributes corresponding to Data, Enterprise, Leadership, Targets, and Analysts.

They also offer the following set of common attributes of people who operate in an analytical culture: They search for the truth; find or identify patterns and get to root causes; are as granular as possible in their analysis; seek data, not just stories, to analyze a question; value negative results as well as positive; use the results of analyses to make decisions and take actions; and are pragmatic about trade-offs in decision making.

But what is known about the analytical culture of colleges and universities? Seeking the truth and being open, honest, and analytical are values often found at the very core of the mission statements of these organizations. And in the faculty ranks, these institutions often have an abundance of skeptics—engaging in critical inquiry, thought, and debate is what faculty members are educated and trained to do within their disciplines. As noted in the previous section, the importance and complexity of measurements associated with teaching and learning also will likely lead to skepticism about quantitative measures in this most important domain of institutional operations.

The key takeaway from this risk category is that organizational culture matters greatly, and patience is required for change. An investment in analytics in a higher education setting should carefully target issues of importance that lend themselves to analytics techniques if such investments are to not only bear fruit but also contribute to the broad acceptance and use of analytics across the institution.

An accurate assessment of the degree to which the campus is data-oriented is an essential first step in mitigating the risk of a countercultural implementation of analytics. Once that step has been accomplished, the DELTA transitions model might serve as a useful guide for cultural change.
The Risk of Saying “No” or “Not Now” to Analytics

The final risk category under the heading of risks for institutional leaders corresponds to a decision to say “no” (or perhaps “not now”) to an investment of time, energy, and financial resources in analytics. Champions of analytics promise better decisions and better results. And there is evidence within the business world that those companies that have developed a data-friendly culture and have made these investments are gaining a strategic advantage over their competitors. In higher education, some institutions are beginning to report success with learning analytics initiatives, leading to significant improvements in retention and learning outcomes. Examples include the work at Rio Salado Community College and the Purdue University Signals Program.26 As noted above, the proper balance of intuitive to analytics-based decision making depends strongly on local culture and context. For schools with the benefit of an excellent reputation, the power of prestige still carries great weight and serves as a barrier to disruptive innovation, as described in The Innovative University.

Historically, higher education has avoided such competitive disruption. There are several reasons for this past immunity. One is the power of prestige in the higher education marketplace, where the quality of the product is hard to measure. In the absence of comparable measures of what universities produce for their students, the well-respected institutions have a natural advantage; because they have been admired in the past, they are presumed to be the best choice for the future.27

For colleges and universities with this advantage, especially when the culture favors decisions based on intuition rather than analytics, the risks of pushing too hard and too soon on analytics may outweigh the risks of decisions based exclusively on intuition. However, the potential inability to respond effectively to a challenging policy environment at the board, state, or federal level; the potential inability to demonstrate institutional efficiency and effectiveness; and/or the potential damaging effects of strategic planning decisions based on “gut instinct” may pose significant risks. For all colleges and universities, the promise and potential of analytics demand attention.

Under the right circumstances, decision making can be enhanced by the tools and techniques of analytics; large data sets, analytics engines, and new data visualization techniques have considerable potential to enhance both student learning and institutional business intelligence. As a result, there is a risk in saying “no” or “not now” to analytics. Will the college fall behind its peers? Will the university miss the opportunity to make better decisions and get better results? The best way to mitigate this risk is to stay informed about analytics initiatives (successes and failures) among peer institutions. EDUCAUSE has compiled an annotated bibliography of analytics resources.
Data and Information Governance Risk

Next, it is important to consider data and information governance and its relationship to risk management. To ensure data and information privacy, security, quality, and auditability, they must be carefully controlled. It is through utilizing risk management that such control can be realized. An effective governance system should involve the entire analytics team—people working at all levels and across the broad array of functional units.

A helpful starting point regarding governance is the “data governance checklist” outlined in table 1, developed by the U.S. Department of Education’s Privacy Technical Assistance Center (http://ed.gov/ptac).²⁸ PTAC was established to provide a “one-stop shop” resource for education stakeholders to learn about privacy, confidentiality, and security practices. While the guidelines were developed for K–12 and include a note that such guidelines for postsecondary education may involve additional considerations outside the scope of the provided list, they are closely connected with FERPA legislation.

Table 1. Data governance checklist

<table>
<thead>
<tr>
<th><strong>Decision-making authority:</strong> Assigning appropriate levels of authority to data stewards and proactively defining the scope and limitations of that authority are a prerequisite to successful data management.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Standard policies and procedures:</strong> Adopting and enforcing clear policies and procedures in a written data stewardship plan is necessary to ensure that everyone in the organization understands the importance of data quality and security—and that staff are motivated and empowered to implement data governance.</td>
</tr>
<tr>
<td><strong>Data inventories:</strong> Conducting an inventory of all data that require protection is a critical step for data security projects. Maintaining an up-to-date inventory of all sensitive records and data systems, including those used to store and process data, enables the organization to target its data security and management efforts. Classifying data by sensitivity helps the data management team recognize where to focus security efforts.</td>
</tr>
<tr>
<td><strong>Data content management:</strong> Closely managing data content, including identifying the purposes for which data are collected, is necessary to justify the collection of sensitive data, optimize data management processes, and ensure compliance with federal, state, and local regulations.</td>
</tr>
<tr>
<td><strong>Data records management:</strong> Specifying appropriate managerial and user activities related to handling data is necessary to provide data stewards and users with appropriate tools for complying with an organization’s security policies.</td>
</tr>
<tr>
<td><strong>Data quality:</strong> Ensuring that data are accurate, relevant, timely, and complete for the purposes they are intended to be used is a high priority issue for any organization. The key to maintaining high-quality data is a proactive approach to data governance that requires establishing and regularly updating strategies for preventing, detecting, and correcting errors and misuses of data.</td>
</tr>
<tr>
<td><strong>Data access:</strong> Defining and assigning differentiated levels of data access to individuals based on their roles and responsibilities in the organization is critical to preventing unauthorized access and minimizing the risk of data breaches.</td>
</tr>
</tbody>
</table>
### Table 1. Data governance checklist (continued)

<table>
<thead>
<tr>
<th><strong>Data security and risk management:</strong> Ensuring the security of sensitive and personally identifiable data and mitigating the risks of unauthorized disclosure of these data is a top priority for an effective data governance plan.</th>
</tr>
</thead>
<tbody>
<tr>
<td>❑ Has a comprehensive security framework been developed, including administrative, physical, and technical procedures for addressing data security issues (such as data access and sharing restrictions, strong password management, regular staff screening and training, etc.)?</td>
</tr>
<tr>
<td>❑ Has a risk assessment been undertaken, including an evaluation of risks and vulnerabilities related to both intentional misuse of data by malicious individuals (e.g., hackers) and inadvertent disclosure by authorized users?</td>
</tr>
<tr>
<td>❑ Is a plan in place to mitigate the risks associated with intentional and inadvertent data breaches?</td>
</tr>
<tr>
<td>❑ Does the organization regularly monitor or audit data security?</td>
</tr>
<tr>
<td>❑ Have policies and procedures been established to ensure the continuity of data services in an event of a data breach, loss, or other disaster (this includes a disaster recovery plan)?</td>
</tr>
<tr>
<td>❑ When sharing data, are appropriate procedures, such as sharing agreements, put in place to ensure that any PII remains strictly confidential and protected from unauthorized disclosure? Note that data sharing agreements must be authorized in applicable local, state, and federal privacy laws and regulations, such as FERPA. These agreements can only take place if data sharing is permitted by law.</td>
</tr>
<tr>
<td>❑ Are appropriate procedures, such as rounding and cell suppression, being implemented to ensure that PII is not inadvertently disclosed in public aggregate reports and that organization’s data reporting practices remain in compliance with applicable local, state, and federal privacy laws and regulations (e.g., FERPA)?</td>
</tr>
<tr>
<td>❑ Are stakeholders, including eligible students or students’ parents, regularly notified about their rights under applicable federal and state laws governing data privacy?</td>
</tr>
</tbody>
</table>

Source: U.S. Department of Education PTAC

In addition to this checklist, the Office of Civil Rights has published draft guidance on risk analysis requirements under the HIPAA Security Rule. The guidance states that “Conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule” and that “All electronic personal health information (e-PHI) created, received, maintained or transmitted by an organization is subject to the Security Rule.”

While the guidance does not prescribe a particular method of risk analysis, it includes several elements of risk analysis that must be incorporated regardless of the method employed.

**Scope of the Analysis**

The scope of risk analysis that the Security Rule encompasses includes the potential risks and vulnerabilities to the confidentiality, availability and integrity of all e-PHI that an organization creates, receives, maintains, or transmits. (45 C.F.R. § 164.306(a).) This includes e-PHI in all forms of electronic media, such as hard drives, floppy disks, CDs, DVDs, smart cards or other storage devices, personal digital assistants, transmission media, or portable electronic media.
Data Collection
An organization must identify where the e-PHI is stored, received, maintained or transmitted. An organization could gather relevant data by: reviewing past and/or existing projects; performing interviews; reviewing documentation; or using other data gathering techniques. The data on e-PHI gathered using these methods must be documented. (See 45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1).)

Identify and Document Potential Threats and Vulnerabilities
Organizations must identify and document reasonably anticipated threats to e-PHI. (See 45 C.F.R. §§ 164.306(a)(2) and 164.316(b)(1)(ii).) Organizations may identify different threats that are unique to the circumstances of their environment. Organizations must also identify and document vulnerabilities which, if triggered or exploited by a threat, would create a risk of inappropriate access to or disclosure of e-PHI. (See 45 C.F.R. §§ 164.308(a)(1)(ii)(A) and 164.316(b)(1)(ii).)

Assess Current Security Measures
Organizations should assess and document the security measures an entity uses to safeguard e-PHI, whether security measures required by the Security Rule are already in place, and if current security measures are configured and used properly. (See 45 C.F.R. §§ 164.306(b)(1), 164.308(a)(1)(ii)(A), and 164.316(b)(1).)

Determine the Likelihood of Threat Occurrence
The Security Rule requires organizations to take into account the probability of potential risks to e-PHI. (See 45 C.F.R. § 164.306(b)(2)(iv).) The results of this assessment, combined with the initial list of threats, will influence the determination of which threats the Rule requires protection against because they are “reasonably anticipated.”

The output of this part should be documentation of all threat and vulnerability combinations with associated likelihood estimates that may impact the confidentiality, availability and integrity of e-PHI of an organization. (See 45 C.F.R. §§ 164.306(b)(2)(iv), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

Determine the Potential Impact of Threat Occurrence
The Rule also requires consideration of the “criticality,” or impact, of potential risks to confidentiality, integrity, and availability of e-PHI. (See 45 C.F.R. § 164.306(b)(2)(iv).) An organization must assess the magnitude of the potential impact resulting from a threat triggering or exploiting a specific vulnerability. An entity may use either a qualitative or quantitative method or a combination of the two methods to measure the impact on the organization.

The output of this process should be documentation of all potential impacts associated with the occurrence of threats triggering or exploiting vulnerabilities that affect the confidentiality, availability and integrity of e-PHI within an organization. (See 45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1)(ii).)

Determine the Level of Risk
Organizations should assign risk levels for all threat and vulnerability combinations identified during the risk analysis. The level of risk could be determined, for example, by analyzing the values assigned to the likelihood of threat occurrence and resulting impact of threat occurrence. The risk level determination might be performed by assigning a risk level based on the average of the assigned likelihood and impact levels.
The output should be documentation of the assigned risk levels and a list of corrective actions to be performed to mitigate each risk level. (See 45 C.F.R. §§ 164.306(a)(2), 164.308(a)(1)(ii)(A), and 164.316(b)(1).)

Finalize Documentation
The Security Rule requires the risk analysis to be documented but does not require a specific format. See 45 C.F.R. § 164.316(b)(1). The risk analysis documentation is a direct input to the risk management process.

Periodic Review and Updates to the Risk Assessment
The risk analysis process should be ongoing. In order for an entity to update and document its security measures “as needed,” which the Rule requires, it should conduct continuous risk analysis to identify when updates are needed. (45 C.F.R. §§ 164.306(e) and 164.316(b)(2)(iii).) The Security Rule does not specify how frequently to perform risk analysis as part of a comprehensive risk management process. The frequency of performance will vary among covered entities. Some covered entities may perform these processes annually or as needed (e.g., bi-annual or every 3 years) depending on circumstances of their environment.

More information about the HIPAA Security Rule as well as risk analysis and risk management is available through the Office for Civil Rights website (http://www.hhs.gov/ocr/privacy/). Also, NIST, the National Institute of Standards and Technology, an agency of the Department of Commerce, provides a series of publications regarding IT security and risk analysis methods. ISO 31000 provides an international standard on the implementation of risk management. Finally, HEISC, the Higher Education Information Security Council, hosted by EDUCAUSE and Internet2, has produced a rich array of relevant resources including frameworks, tools, lists of consultants, and sample RFPs.

As noted in the overview of risk management above, an important part of the process is to make an assessment of data sensitivity. Classifying data value, a closely related concept, is addressed in the appendix to this guide. HEISC has created a “risk management framework” that provides a high-level overview of the process for conducting risk assessment of information systems within higher education. Included in that overview is a “starter set of risk assessment criteria for identifying (and classifying) data assets,” as shown in table 2.
Table 2: Data sensitivity classification

<table>
<thead>
<tr>
<th>Legal requirements</th>
<th>Most Critical</th>
<th>Critical</th>
<th>Least Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Highest level of sensitivity</td>
<td>Moderate level of sensitivity</td>
<td>Very low, but still requiring some protection</td>
</tr>
<tr>
<td>Protection of data is required by law (e.g., HIPPA and FERPA data elements and other PII protected by law)</td>
<td>The institution has a contractual obligation to protect the data (e.g., bibliographic citation data, bulk licensed software)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reputational risk</th>
<th>High</th>
<th>Medium</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information that provides access to resources, physical or virtual</td>
<td>Smaller subsets of Most Critical data from a school, large part of a school, or department</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Other institutional risks</th>
<th>Medical Student Prospective student Personnel Donor or prospect Financial Contracts Physical plant detail Credit card numbers Certain management information</th>
<th>Information resources with access to Most Critical data Research detail or results that are not Most Critical Library transactions (e.g., catalog, circulation, acquisitions)</th>
<th>Financial transactions that do not include Most Critical data (e.g., telephone billing) Very small subsets of Most Critical data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Campus maps</td>
<td>Personal directory data (e.g., contact information) E-mail</td>
<td>Institutionally published data</td>
<td></td>
</tr>
</tbody>
</table>

For an organization that values data-informed decision making in its institutional governance approach, data and information governance is integral and essential. Effective data and information governance sets the stage for effective analytics, which in turn supports effective organizational governance through its focus on both quality and control, leading to “good data” on which accurate, appropriate decisions can be based.
Data and information governance risk can be mitigated with carefully conceived and well-written policy documents. And it is through the utilization of risk management principles and processes that appropriate levels of control can be realized. The data governance checklist associated with FERPA, the risk analysis elements from HIPAA guidance, and the EDUCAUSE resources highlighted in this section all serve as good guidelines for policy development and risk management.

Data and Information Quality Risk

You can’t be analytical without data, and you can’t be really good at analytics without really good data. (Thomas Davenport, Jeanne Harris, and Robert Morison, Analytics at Work: Smarter Decisions, Better Results [Cambridge, MA: Harvard Business School Press, 2010], 23)

We don’t have too much information. Its quantity and rapid growth is not a problem. In fact, it represents a wealth of potential. The problem is that most of us don’t know how to dive into this ocean of information, net the best of it, bring it back to shore, and sort it out—that is, understand it well enough to make good use of it. (Stephen Few, Now You See IT: Simple Visualization Techniques for Quantitative Analysis [Oakland: Analytics Press, 2009], 1)

Excellence in statistical graphics consists of complex ideas communicated with clarity, precision, and efficiency…. What is to be sought in designs for the display of information is clear portrayal of complexity. Not the complication of the simple; rather the task of the designer is to give visual access to the subtle and the difficult—that is the revelation of the complex. (Edward Tufte, The Visual Display of Quantitative Information [Cheshire, CT: Graphics Press, May 2001], 13, 191)

This section highlights some key ideas about data quality and data visualization from the authors quoted above, along with similarly relevant insights from an often-cited scholarly paper on data quality assessment. Pipino, Lee, and Wang provide a list of 16 data quality dimensions (see table 3) and note that those interested in data quality assessment must consider not only objective measures of data quality but also the subjective perceptions of those who will use them.35 They suggest several ways to quantify objective metrics. For example, one might compute 1 minus the ratio of the number of missing data points divided by the total number of data points. The result would be 1 for a complete set and <1 in the case of missing data. These
authors recommend development of both objective and subjective (survey-based) metrics for chosen data dimensions and then a process for comparing results and taking necessary actions to resolve differences and improve data quality.

Table 3. Dimensions of data quality

<table>
<thead>
<tr>
<th>Dimensions</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accessibility</td>
<td>The extent to which data are available or easily and quickly retrievable</td>
</tr>
<tr>
<td>Appropriate amount of data</td>
<td>The extent to which the volume of data is appropriate for the task at hand</td>
</tr>
<tr>
<td>Believability</td>
<td>The extent to which data are regarded as true and credible</td>
</tr>
<tr>
<td>Completeness</td>
<td>The extent to which data are not missing and are of sufficient breadth and depth for the task at hand</td>
</tr>
<tr>
<td>Concise representation</td>
<td>The extent to which data are compactly represented</td>
</tr>
<tr>
<td>Consistent representation</td>
<td>The extent to which data are presented in the same format</td>
</tr>
<tr>
<td>Ease of manipulation</td>
<td>The extent to which data are easy to manipulate and apply to different tasks</td>
</tr>
<tr>
<td>Free-of-error</td>
<td>The extent to which data are correct and reliable</td>
</tr>
<tr>
<td>Interpretability</td>
<td>The extent to which data are in appropriate languages, symbols, and units, and the definitions are clear</td>
</tr>
<tr>
<td>Objectivity</td>
<td>The extent to which data are unbiased, unprejudiced, and impartial</td>
</tr>
<tr>
<td>Relevancy</td>
<td>The extent to which data are applicable and helpful for the task at hand</td>
</tr>
<tr>
<td>Reputation</td>
<td>The extent to which data are highly regarded in terms of source and content</td>
</tr>
<tr>
<td>Security</td>
<td>The extent to which access to data is restricted appropriately to maintain their security</td>
</tr>
<tr>
<td>Timeliness</td>
<td>The extent to which the data are sufficiently up-to-date for the task at hand</td>
</tr>
<tr>
<td>Understandability</td>
<td>The extent to which data are easily comprehended</td>
</tr>
<tr>
<td>Value-added</td>
<td>The extent to which data are beneficial and provide advantages for their use</td>
</tr>
</tbody>
</table>

In addition to the quality dimensions already listed above, Davenport et al. highlight the value of data uniqueness in providing a competitive advantage as well as that of data integration such an ERP system provides. They note that achieving complete data integration is a goal unlikely to be achieved, but that it is important for the data that matter most; one version of the truth is very helpful in such cases. Data access, privacy, and governance are also noted as essential elements of “good data.”

While the terms *data* and *information* are sometimes used interchangeably, this guide defines *information* as meaningful patterns of data that communicate and promote understanding of the complex, as noted by Edward Tufte above. Stephen Few lists the following traits of meaningful data:

- **High volume**—increases the likelihood that there will be sufficient data to explore questions being pursued
• **Historical**—understanding how information changes with time often provides valuable insight
• **Consistent**—when things do change over time, it’s important to keep data consistent
• **Multivariate**—more variables at hand when trying to make sense of data increases the likelihood of discovery of meaningful patterns
• **Atomic**—analysts need the ability to slice and dice data to the lowest level
• **Clean**—accurate, free-of-error, and complete
• **Clear**—expressed in familiar, understandable terms
• **Dimensionally structured**—data organized into dimensions (categorical data such as departments, regions, or year) and measures (the quantitative data itself)
• **Richly segmented**—data presorted into meaningful groups
• **Of known pedigree**—how it came to be, where it came from, and what calculations might have been used to create [it]

Tufte is well-known for his books on data visualization (see recommended readings 13–15). In *Envisioning Information*, he writes, “The principles of information design are universal—like mathematics—and are not tied to unique features of a particular language or culture.” These books provide many examples of effective and not-so-effective data visualization, along with statements and explanations of design principles.

To draw on a Ford Motor Company slogan, in analytics work “quality is job one.” Within the computer science and information technology communities, the expressions “garbage in, garbage out” or “garbage in, gospel out” (GIGO) have long been used as cautions for programmers and users of data and information produced by machines. Clearly, data and information of poor quality may lead to poor decisions; this can be devastating for an organization that wants to use analytics effectively and develop a culture of analytics.

Data and information governance is essential for mitigating the risks of poor quality. A group of data stewards should be assigned these tasks:

- Develop an inventory of institutional data and information.
- Ensure that there are clear definitions and quality standards for all data and information.
- Establish and exercise a data and information quality review and improvement process targeting those data and information elements that matter most.

The *International Association for Information and Data Quality* and the *Association for Institutional Research* are recommended resources for those interested in making professional connections and doing research in this area.
Data and Information Compliance Risk

The compliance obligations of colleges and universities are vast and growing, and the pressure on institutions from both external and internal sources to implement, monitor, and improve institutional compliance programs continues unabated. In an era of budget cuts and limited resources yet growing regulation, designing and implementing effective compliance programs to track, monitor, and update the most important compliance duties and risks is daunting indeed. It is a task shared by a wide range of institutional officials, including general counsel, compliance officers, risk managers, auditors, and an entire array of administrators with primary responsibility for compliance in their own departments or divisions. (Program description of “College and University Compliance Programs,” a NACUA Workshop, in collaboration with EDUCAUSE, November 9–11, 2011, Washington, D.C.)

Recall that compliance means conforming to the requirements of an authorized and recognized external agent—usually associated with a law (state, federal, or international) or contractual agreement—or, as ISO 27002 indicates, enforcing internal policies. The relationship between compliance and risk management is due to the fact that a failure to comply can lead to an adverse result such as a financial penalty, additional work, or even personal liability and imprisonment for institutional officers. Those in governance roles must decide how to allocate resources for compliance to achieve an acceptable level of risk. Compliance risk is quite tangible, as evidenced by statistics from the Privacy Rights Clearinghouse. This organization has records of 133 incidents between 2007 and 2011 involving unintended public disclosure of sensitive information by educational institutions; each of those disclosures had the potential to (and in some cases most likely did) expose the institution to legal (state and/or federal), financial, and/or reputational liabilities. Investing in compliance work will not only reduce the risk of such incidents but will also likely reduce the risks of analytics, because those investments will increase data and information awareness, quality, and protection.

Higher education today faces many sources of compliance requirements. The relevance of FERPA, HIPAA, and GLB have already been noted. The Sarbanes-Oxley Act, known as SOX, also applies in a limited fashion. NACUBO, the National Association of College and University Business Officers, has released an advisory report recommending that colleges and universities consider SOX “as a framework to help evaluate overall financial risks, and not simply comply with accountability concepts that stem from structures, and circumstances that differ fundamentally from the stewardship responsibilities and public obligations they face.”

38

39
Potential requirements are also associated with state data-breach laws. Forty-six states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information (see the National Conference of State Legislatures website for an up-to-date list of such laws).

The Red Flags Rule is a component of FACT, the Fair and Accurate Credit Transactions Act, signed into law in December 2010. Section 114 of the act requires agencies that regulate financial institutions and businesses to jointly develop a set of rules to mandate the detection, prevention, and mitigation of identity theft. Because of the increased use of credit cards in college and university transactions, compliance with the security guidelines of the Payment Card Industry (PCI) is yet another dimension of data and information security.

Two key takeaways from the various compliance requirements are:

- Not only is data and information quality a requirement, so is auditability, i.e., data must be tracked and verified at every step in their life cycle.
- Processes and procedures must be in place to ensure data and information privacy and security.

In this sea of confusing and complex requirements, where does one go for help? Useful frameworks for thinking about or establishing data and information control systems, including matters of compliance, can be found in several ISO/IEC (International Organization for Standardization/International Electrotechnical Commission) standards. For example, ISO/IEC 27002 regarding information security contains guidance on the following 11 topics:

- **Security policy** — management direction
- **Organization of information security** — governance of information security
- **Asset management** — inventory and classification of information assets
- **Human resources security** — security aspects for employees joining, moving, and leaving an organization
- **Physical and environmental security** — protection of the computer facilities
- **Communications and operations management** — management of technical security controls in systems and networks
- **Access control** — restriction of access rights to networks, systems, applications, functions, and data
- **Information systems acquisition, development, and maintenance** — building security into applications
- **Information security incident management** — anticipating and responding appropriately to information security breaches
- **Business continuity management** — protecting, maintaining, and recovering business-critical processes and systems
• **Compliance**—ensuring conformance with information security policies, standards, laws, and regulations

Another frequently cited source for establishing and organizing data and information controls for compliance within an IT environment is COBIT, published by the IT Governance Institute (http://www.itgi.org/).

A final resource of special importance regarding compliance in higher education environments is the Higher Education Compliance Alliance, of which EDUCAUSE is a member. This coalition “was created to provide the higher education community with a centralized repository of information and resources for compliance with federal laws and regulations. Spearheaded by the National Association of College and University Attorneys (NACUA), the Compliance Alliance is now comprised of 22 participating associations representing a broad cross-section of higher education interests.”

Many resources at this site are freely available, and others are accessible to association members via a password.

---

**Investing in compliance work will likely reduce the risks of analytics by increasing data and information awareness, quality, auditability, and protection. Those in college and university governance roles must decide how to allocate resources for compliance to achieve an acceptable level of risk. Has your institution made necessary and sufficient investments in compliance work? The Higher Education Compliance Alliance is a good source to help you answer this question.**

---

**Special Topics in Risk Management**

**Institutional Use of Data for Learning Analytics**

A byproduct of the Internet, computers, mobile devices, and enterprise learning management systems (LMSs) is the transition from the ephemeral to captured, explicit data. Listening to classroom lecture or reading a book leaves limited trails. A hallway conversation essentially vaporizes as soon as it is concluded. However, every click, every tweet or Facebook status update, every social interaction, and every page read online can leave a digital footprint. Additionally, online learning, digital student records, sensors, and mobile devices now capture rich data trails and activity streams. These learner-produced data trails provide valuable insight into what is actually happening in the learning process and suggest ways in which educators can make improvements. (Phil Long and George Siemens, “Penetrating the Fog: Analytics in Learning and Education,” EDUCAUSE Review 46, no. 5 [September/October 2011], 32)
In the section on risks for institutional leaders, a caution was made regarding important but complex measurement issues such as the assessment of student learning outcomes. As suggested in the quote above, new technologies and recent research in the areas of educational data mining and learning analytics are providing new insights about how students, courses, and academic programs “learn.”

SoLAR, the Society for Learning Analytics Research (http://www.solaresearch.org), defines learning analytics as follows:

Learning analytics (LA) is the measurement, collection, analysis and reporting of data about learners and their contexts, for purposes of understanding and optimizing learning and the environments in which it occurs. Learning analytics are largely concerned with improving learner success.43

Figure 4 shows the interrelationships of the elements that support learning analytics.44

The benefits that have been articulated for learning analytics include:

- Reduced attrition through early detection of at-risk students and the ability to generate alerts for learners and educators.
- Personalized and adapted learning process and content, ensuring that each learner receives resources and teaching that reflect their current knowledge state.
- Extended and enhanced learner achievement, motivation, and confidence by providing learners with timely information about their performance and that of their peers, as well
as providing suggestions on activities and content that address identified knowledge gaps.

- Better use of teacher time and effort by providing information on which students need additional help, which students are candidates for mentoring others, and which teaching practices are making the biggest impact.
- Higher-quality learning design and improved curriculum development processes through the utilization of data generated during real-time instruction and learning activities.
- Interactive visualizations of complex information give learners and educators the ability to “zoom in” or “zoom out” on data sets, depending on the needs of a specific teaching or learning context.
- More rapid achievement of learning goals by giving learners access to tools that help them evaluate their progress and determine which activities are producing the best results.

While there is considerable interest in and developing research activity in both learning analytics and educational data mining, the collection and use of “data trails” as described above does generate questions about their ethical use. For those interested in contributing to the conversation about these issues, SoLAR has established a collaboration space (in Google Docs) for the discussion and development of guidelines, which allows anyone to contribute or edit without signing in. Following is a summary of the discussion as of the writing of this guide:

The collection of all data, whether formal course activities, supporting/related activity streams or additional profile data is analyzed for the purpose of better understanding the learner’s needs and their performance level in order to better support their learning process to drive success (at the individual learner level, which then builds to course, instructor(s), programs, departments, schools, districts…). All analytics should be done in the spirit of this goal and other uses of the data in its collection, sharing, or analysis is not in compliance with the principles of the analysis program of the institution. Any party participating in uses or practices not aligned with these goals or contrary to them are subject to disciplinary review and action, up to and including criminal prosecution.

- Don’t assume that your users don’t care about privacy no matter what they do on Facebook or Twitter that seems to indicate so.
- No matter who owns the data (the student, the institution, or the system vendor), it should not be released to a third party for marketing purposes.
- Transparency so that the learner has the right to know who is collecting the data, what data is collected, for what purpose(s) it is being collected, how the data will be used, and how to access data about themselves.
- Transparency so the learner has a right to easily understandable and accessible information about privacy and security practices.
- Data must be kept secure at many levels—such as with HIPPA where certain “levels” of administration and specific assignment give very specific access to information.
- Data must be reviewable by the learner to ensure privacy.
However, a number of questions remain: Should students have the ability to opt-out of having their data collected? What is the recourse for individuals who have had their data misused or inappropriately shared? Who owns the data mined from a learning process? Who sees the outcome of analytics, and to what level of detail? Who owns the intervention algorithms, and who can modify them? Does the student have a right to see and understand the basis for interventions?

For the purposes of this guide, caution is advised regarding the collection and use of data trails associated with learning-analytics initiatives. The guidelines and questions listed above might serve as a useful starting point, and, in any case, compliance with FERPA, HIPAA, and GLB requirements should be a primary consideration.

Third Parties—Cloud and Software-as-a-Service Issues (includes sample contract terms and conditions)

The increasing use of cloud services and SaaS strategies in higher education has generated a considerable amount of discussion around related security issues. Thomas Trappler provides an especially helpful overview of the contract negotiation and management issues related to the use of such services. He includes the following high-level guidelines for such arrangements.

Ensure that your contract with a cloud service provider:

- Codifies the specific parameters and minimum levels required for each element of the service, as well as remedies for failure to meet those requirements.
- Affirms your institution’s ownership of its data stored on the service provider’s system, and specifies your rights to get it back.
- Details the system infrastructure and security standards to be maintained by the service provider, along with your rights to audit their compliance.
- Specifies your rights and cost to continue and discontinue using the service.

Trappler notes that while there are variations of cloud computing, e.g., software as a service (SaaS), infrastructure as a service (IaaS), and platform as a service (PaaS), the contract issues associated with each are similar and typically fall into one of the four categories above. His article provides guidance on each of the topics shown in bullets in figure 5.
Figure 5. Key considerations in third-party service contracts

He concludes his article by emphasizing the importance of a positive collaboration between IT end-user units, legal counsel, policy experts, and the procurement office on your campus. More details about these working relationships can be found in recommended reading 16.

With regard to outsourced services, Marty Ringle, chief technology officer at Reed College in Portland, Oregon, states:

I’ve dealt with each cloud (and other outsource) contract individually and reworked the language to meet my concerns du jour (which are ever changing). The primary common denominator is that I generally get the provider:

1. To bind themselves to the same federal and state restrictions as the college, as if they were functioning as an employee or agent of the college (that means they take on the obligations of FERPA, HIPAA, the Oregon ID Theft Protection Act, etc.).
2. To agree that Reed-provided data shall be used exclusively for the purpose(s) outlined in the agreement and for no other purpose(s).
3. To agree that such data shall not in any way be made accessible to anyone except employees (or subcontractors) who must have access to the data in order to fulfill the commitments of the agreement and then only upon condition that they are aware of and bound to the privacy and confidentiality terms of the agreement.49

In 2010, the Commons Solutions Group and NACUA jointly created sample language for RFP and contract documents that might serve as a basis for cloud or other outsourced services. For the purposes of this guide, just a few examples are provided of contract language from the model contract related to risk factors associated with analytics initiatives. The reader is strongly encouraged to take advantage of these helpful resources and to review them in their entirety.50
Data Privacy

a. Vendor will use Customer Data and End User Data only for the purpose of fulfilling its duties under this Agreement and for Customer’s and its End User’s sole benefit, and will not share such data with or disclose it to any third party without the prior written consent of Customer or as otherwise required by law. By way of illustration and not of limitation, Vendor will not use such data for Vendor’s own benefit and, in particular, will not engage in “data mining” of Customer or End User Data or communications, whether through automated or human means, except as specifically and expressly required by law or authorized in writing by Customer.

b. [depending on nature of services and data at issue] All Customer and End User Data will be stored on servers, located solely within the Continental United States.

c. Vendor will provide access to Customer and End User Data only [to] those Vendor employees and subcontractors who need to access the data to fulfill Vendor’s obligations under this Agreement. Vendor will ensure that employees who perform work under this Agreement have read, understood, and received appropriate instruction as to how to comply with, the data protection provisions of this Agreement, and have undergone all background screening and possess all qualifications required by Customer [alternative: “undergone all background screening and possess all qualifications appropriate to the nature of the employees’ duties and the sensitivity of the data they will be handling,”] prior to being granted access to the Data.

Data Integrity

Vendor will take commercially reasonable measures, including regular data integrity audits, to protect Customer and End User Data against deterioration or degradation of data quality and authenticity.

Response to Legal Orders, Demands, or Requests for Data

a. Except as otherwise expressly prohibited by law, Vendor will:

   (i) immediately notify Customer of any subpoenas, warrants, or other legal orders, demands or requests received by Vendor seeking Customer and/or End User Data;

   (ii) consult with Customer regarding its response;

   (iii) cooperate with Customer’s reasonable requests in connection with efforts by Customer to intervene and quash or modify the legal order, demand or request; and

   (iv) upon Customer’s request, provide Customer with a copy of its response.

b. If Customer receives a subpoena, warrant, or other legal order, demand or request seeking Customer or End User Data maintained by Vendor, Customer will promptly provide a copy to Vendor. Vendor will promptly supply Customer with copies of data required for Customer to respond, and will cooperate with Customer’s reasonable requests in connection with its response.

Data Retention and Disposal

a. Vendor will use commercially reasonable efforts to retain data in an End User’s account, including attachments, until the End User deletes them or for an alternative time period mutually agreed by the parties.

b. Using appropriate and reliable storage media, Vendor will regularly back up Customer and End User Data and retain such backup copies for a minimum of
[timeframe]. At the end of that time period and at Customer’s election, Vendor will either securely destroy or transmit to Customer repository the backup copies. Upon Customer’s request, Vendor will supply Customer a certificate indicating the records destroyed, the date destroyed, and the method of destruction used.

c. Vendor will retain logs associated with End User activity for a minimum of [x period of time], unless the parties mutually agree to a different period.

d. Vendor will immediately place a “hold” on the destruction under its usual records retention policies of records that include Customer and End User Data, in response to an oral or written request from Customer indicating that those records may be relevant to litigation that Customer reasonably anticipates. Oral requests by Customer for a hold on record destruction will be reduced to writing and supplied to Vendor for its records as soon as reasonably practicable under the circumstances. Customer will promptly coordinate with Vendor regarding the preservation and disposition of these records. Vendor shall continue to preserve the records until further notice by Customer.31

The data and information envisioned for use in learning analytics present new ethical issues for faculty and staff. Also, increasing use of learning analytics, cloud services, and software as a service in higher education is resulting in new governance challenges and new risk factors. Ultimately the data-owning organization cannot abrogate responsibility for data protection. EDUCAUSE provides helpful resources for such issues, including the CSG-NACUA Shared Services Working Group Model Contract and an annotated analytics bibliography.

Conclusion

This guide has provided an introduction and overview of major risk categories for an institution considering investments of time, energy, and money in analytics work. High-quality data and information (meaningful patterns of data) are essential for success, as is a data-friendly culture. It is important to have an understanding of the balance of intuitive and analytics-based decision making that corresponds to the local culture. Major and explicit risks are associated with data privacy and security as a result of various federal and state compliance requirements, as well as any internal policy requirements. In addition, special care and expertise are needed for managing outsourced (cloud or SaaS) services. In the case of the developing research area of learning analytics, questions remain about the ethical use of data—a general understanding of these issues is still in development.

In Analytics: The Widening Divide, three key competencies in organizations that have been most successful with analytics are identified.32 These competencies are recommended as a concise summary of developmental objectives for colleges and universities that choose to invest in analytics.
1. **Information management**: the use of methodologies, techniques, and technologies that address data architecture, transformation, movement, storage, integration, and governance of enterprise information and master data management.

2. **Analytical skills and tools**: enhance performance by applying advanced techniques such as modeling, deep computing, simulation, data analytics, and optimization to improve efficiency and guide strategies that address specific business processes.

3. **Data-oriented culture**: a pattern of behaviors and processes by a group of people who share a belief that having, understanding, and using certain kinds of data and information plays a critical role in the success of their organization.

The focus in this guide has been on the risks of such an investment. Successful and effective analytics work requires an enterprise-wide perspective—this is a team “sport.” Figure 6, adapted from *Business Analytics for Managers*, illustrates how those serving across the full spectrum of roles in college and university environments might work together for this purpose.

![Figure 6](image-url)  
**Figure 6. Organizing for effective analytics practice in higher education**

While all the roles illustrated above are important, the faculty, analyst, and report developer roles—those who routinely practice the art of converting data to meaningful information that can be used to illuminate the complex and to enhance decision making—has been highlighted. An article by EDUCAUSE Vice President Susan Grajek on the past, present, and future of research, data, and analytics in higher education technology provides a summary of ongoing EDUCAUSE actions to achieve such a vision and advocates the professionalization of IT data,
research, and analytics work. At the end of the day, it will be people with a deep understanding of institutional processes, a balance of both technical and human relationship skills, and a love and talent for teaching (or coaching) that will minimize the risks of analytics work and maximize its results.54
Appendix

Additional Risk Management Considerations

Following are excerpts and highlights from David Hill’s book Data Protection: Governance, Risk Management, and Compliance (recommended reading 12). This book is recommended for those who want to develop a deeper understanding of the GRC framework and to pursue risk management processes in the context of data protection.

**Business continuity versus disaster recovery:** “If IT organizations do not understand that day-to-day operations and disaster recovery planning have different requirements for both physical and logical data protection, they may not have the right technology mix—and therefore they make the wrong investments for data protection…. If disaster recovery is like responding to an epidemic, then operational recovery is like responding to events in an emergency room.”

Business continuity in day-to-day operations requires functional hardware, software, data storage systems, and networks. Application software should be prioritized and system downtime should be monitored. If redundancy is built into such systems to provide resiliency, then individual components may fail without an interruption in service. Special attention should be paid to data storage because, as Hill notes, “reloading an application, hot-swapping a server, or rerouting messages along a network” can often be accomplished in a matter of minutes, while recovering or reloading data will likely take much longer.

Hill also notes that the Storage Network Industry Association (SNIA) defines disaster recovery as “the recovery of data, access to data and associated processing through a comprehensive process of setting up a redundant site (equipment and work space) with recovery of operational data to continue business operations after loss of use of all or part of a data center.” Estimates of the probability of a disaster and associated recovery time may be difficult to determine but will likely have a high degree of impact and thus are important.

**Defining objectives:** “The objectives that an organization should consider are data availability, data preservation, data responsiveness (i.e., getting the data to the user within a reasonable time), and data confidentiality.” Hill recommends keeping these objectives in balance because too much focus on any one may have a negative impact on the others. Also, investments in data storage can benefit all three of these objectives assuming one or more copies of the data are available.

**Physical and logical data:** “Operational and disaster continuity require the proper level of both physical (storage device level) and logical (the data itself) data protection.” Risk management analysis should account not only for the possibility of hardware failure, e.g., damaged or destroyed hard drives, but also that of data corruption and corresponding downtimes for both.
Classifying data value: Data need to be protected because of their value in institutional operations as well as the potential negative consequences of loss, corruption, or falling into the wrong hands. As a result, any risk management approach should include a process of data classification. First, consider data value. Hill notes that the SNIA has defined important terms related to this classification as follows:

- **Recovery point objective (RPO):** the maximum acceptable time period prior to a failure or disaster during which changes to data may be lost as a consequence of recovery. Data changes preceding the failure or disaster by at least this time period are preserved by recovery. Zero is a valid value and is equivalent to a “zero data loss” requirement.
- **Recovery time objective (RTO):** The maximum acceptable time period required to bring one or more applications and associated data back from an outage to a correct operational state.
- **Data protection window (DPW):** Like the backup window, this is the available time during which a system can be quiesced and the data can be copied to a redundant repository without impacting business operations.

The table that follows shows how an organization might classify and quantify these concepts.

<table>
<thead>
<tr>
<th>Data Value Class</th>
<th>Data Availability</th>
<th>RPO (data loss risk)</th>
<th>RTO (max recovery time)</th>
<th>DPW (copy data time)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Not important for operations</td>
<td>90%</td>
<td>1 week</td>
<td>7 days</td>
<td>Days</td>
</tr>
<tr>
<td>Important for productivity</td>
<td>99%</td>
<td>1 day</td>
<td>1 day</td>
<td>12 hours</td>
</tr>
<tr>
<td>Business important information</td>
<td>99.9%</td>
<td>2 hours</td>
<td>2 hours</td>
<td>10 minutes</td>
</tr>
<tr>
<td>Business vital information</td>
<td>99.99%</td>
<td>10 minutes</td>
<td>15 minutes</td>
<td>None</td>
</tr>
<tr>
<td>Mission-critical information</td>
<td>99.999%</td>
<td>1 minute</td>
<td>1.5 minutes</td>
<td>None</td>
</tr>
</tbody>
</table>
Degrees (or Layers) of Protection

Following from the concepts of levels of data value is the notion of levels (or degrees) of data protection. The following table illustrates how one might think about such degrees for both physical and logical data and for both operational and disaster continuity.

Table A.2. Degrees of protection

<table>
<thead>
<tr>
<th>Physical</th>
<th>Operational Continuity</th>
<th>Disaster Continuity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Higher availability</td>
<td>Higher availability</td>
</tr>
<tr>
<td>Degree 1: RAID/local mirroring</td>
<td>Degree 1: Remote mirroring</td>
<td></td>
</tr>
<tr>
<td>Degree 2: Remote mirroring</td>
<td>Degree 2: Remote dated replication</td>
<td></td>
</tr>
<tr>
<td>Lower availability</td>
<td>Lower availability</td>
<td></td>
</tr>
<tr>
<td>Degree 3: Tape/disk-based backup</td>
<td>Degree 3: Vaulted tapes</td>
<td></td>
</tr>
<tr>
<td>Logical</td>
<td>Higher availability</td>
<td>Higher availability</td>
</tr>
<tr>
<td>Degree 1: Continuous data protection</td>
<td>Degree 1: Continuous data protection</td>
<td></td>
</tr>
<tr>
<td>Degree 2: Point-in-time copy</td>
<td>Degree 2: Remote dated replication</td>
<td></td>
</tr>
<tr>
<td>Lower availability</td>
<td>Lower availability</td>
<td></td>
</tr>
<tr>
<td>Degree 3: Disk-based backup</td>
<td>Degree 3: Vaulted tapes</td>
<td></td>
</tr>
<tr>
<td>Degree 4: Tape-based backup</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Information life-cycle management (ILM): The value and sensitivity of data and information not only depend on type but also are a function of time. ILM is “the policy-driven management of data and information as it changes value throughout the full range of its life cycle from conception to disposition.”

Following are four key definitions related to ILM:

- **Tiering** is the separation of storage into classes by the characteristics of the storage itself: performance (speed and availability), functional capabilities, and cost. Tiering is a storage device–related concept.

- **Pooling** refers to a collection of information that is managed as a homogenous whole for quality of service purposes, such as response time and availability. Pooling is an information-related process. The objective is to map a pool of information to a choice of storage tier, and the net result is a storage pool.

- A data **archive** is “a consistent copy of a collection of data, usually taken for the purpose of a business application state.” Archives are normally used for auditing and analysis rather than for application recovery. After files are archived, online copies of them are typically defended and must be restored by explicit action.

- **Active versus deep archiving**: Active archiving is about managing fixed-content production data which has been kept online for possible retrieval. In the case of deep
archiving, data are stored offline because there is little chance that the data will ever need to be accessed again.

Data Protection Technologies
Hill also provides useful information about major categories of data protection technologies and how those technologies might fit into an overall data protection framework. The following table is an example.

Table A.3. Data protection technologies

<table>
<thead>
<tr>
<th></th>
<th>Operational Continuity</th>
<th>Disaster Continuity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Active Changeable</td>
<td>Active Archive</td>
</tr>
<tr>
<td>Physical</td>
<td>RAID</td>
<td>RAID</td>
</tr>
<tr>
<td></td>
<td>Cloned point-in-time copy</td>
<td>Dated replication</td>
</tr>
<tr>
<td></td>
<td>Tape automation</td>
<td>WORM tape</td>
</tr>
<tr>
<td></td>
<td>Virtual tape library</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Continuous data protection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Data protection appliance</td>
<td></td>
</tr>
<tr>
<td>Logical</td>
<td>Point-in-time copy</td>
<td>WORM disk</td>
</tr>
<tr>
<td></td>
<td>Tape automation</td>
<td>Guaranteed uniqueness</td>
</tr>
<tr>
<td></td>
<td>Virtual tape library</td>
<td>Electronic locking</td>
</tr>
<tr>
<td></td>
<td>Continuous data protection</td>
<td>Dated replication</td>
</tr>
<tr>
<td></td>
<td>Scheduled image protection</td>
<td>WORM tape</td>
</tr>
<tr>
<td></td>
<td>Data protection appliance</td>
<td>Compliance appliance</td>
</tr>
</tbody>
</table>

Strategies for Protection of Confidential Data and Information. One of the greatest data protection risks an organization faces is loss of control of confidential or highly sensitive data and information. There are three approaches to mitigate these risks, which can and should be used in conjunction with one another:

- Limiting access to sensitive information only to authorized users. This approach relies on effective access control and identity management systems and is infrastructure-focused.
- Limiting the uses of sensitive information to only authorized uses. This approach relies on policy for effectiveness.
- By rendering sensitive information unusable to those who are unauthorized, even if they somehow obtain a copy of the information. This approach relies on encryption.
eDiscovery: “Why should data governance receive so much attention? The changes to the Federal Rules of Civil Procedure (FRCP) that became effective on December 1, 2006, are the tipping point in making a formal data governance strategy, policy, and process mandatory, because they apply to any enterprise that can be used in the U.S. federal court system… the FRPC rules govern the discovery process for civil litigation, which decrees how an enterprise must provide legitimately requested information to requesting parties in a civil litigation case…. Electronic discovery (eDiscovery) is the process used for making available electronic records.”

Conceiving and managing a formal and effective eDiscovery process is an important risk mitigation strategy because failure to comply with FRCP rules can lead to fines and sanctions. Hill provides an overview of the Electronic Discovery Reference Model (EDRM)—an existing framework for eDiscovery processes.
Acknowledgments

The author wishes to thank David Hill for his permission to reprint sections of *Data Protection: Governance, Risk Management, and Compliance* in the appendix.

Recommended Readings


Notes


3 Ibid.


7 Shah et al., “Good Data Won’t Guarantee Good Decisions.”


9 Davenport et al., Analytics at Work.


11 See, for example, the CSG-NACUA Shared Services Working Group Model Contract (http://www.educause.edu/Modelcontract) and the annotated analytics bibliography (http://net.educause.edu/ir/library/pdf/PUB9010.pdf).


13 Kiron et al., Analytics: The Widening Divide.


18 Davenport et al., Analytics at Work.

19 Ibid.

20 Ewel, “Assessment, Accountability, and Improvement.”

21 Christensen and Erying, The Innovative University, 390.


24 Kiron et al., Analytics: The Widening Divide.

25 Davenport et al., Analytics at Work.

26 See note 8.

27 Christensen and Erying, The Innovative University, 17.


32 See note 16.

33 HEISC resources are available through the EDUCAUSE Library at http://www.educause.edu/library/security-risk-assessment-and-analysis.

34 The risk management framework is available at https://wiki.internet2.edu/confluence/display/itsg2/Risk+Management+Framework.


36 Davenport et al., Analytics at Work.
Few, Now You See It.


Ibid.


See “Learning Analytics: Guidelines for Ethical Use” at https://docs.google.com/document/d/1b8RCyldBoslywDhNlgb9f4k7-hL_Uzui3HUx7IBUDzQ/edit.


Marty Ringle (CIO, Reed College), in a discussion with the author, March 2012.

See the CSG-NACUA Shared Services Working Group’s model RFP (http://net.educause.edu(elements/attachments/ModellRFP.pdf), model contract (http://net.educause.edu(elements/attachments/ModelContract.pdf), and table of related issues (http://net.educause.edu(elements/attachments/ModelIssues.pdf) from July 2010.

CSG-NACUA model contract, 4–7.

Kiron et al., Analytics: The Widening Divide.
