

Colorado School of Mines Compliance Risk Assessment: 2011



Colorado School of Mines

Entity-wide Compliance Risk Assessment

Contents

Section 1 – Executive Summary.....	4
Overview	4
The Report.....	5
Purpose, Scope and Methodology	5
Strengths CSM Brings to the Compliance Environment.....	7
Opportunities for Improving the Compliance Infrastructure	8
Identification of Risk Areas.....	10
Section 2 – Key Risk Areas.....	13
Research.....	13
Federal Grants	15
Professional Consulting Contracts.....	18
University Advancement.....	20
Protecting the Rights of Faculty, Staff and Students	21
Protection of Personally Identifiable Information.....	23
Section 3 – Functional Areas/ Compliance Partners	26
Academic Affairs.....	28
Admissions	34
Athletics.....	36
Finance & Administration.....	39
Financial Aid.....	43
Graduate Studies	49
Human Resources	52
Information Technology.....	59
Plant Operations.....	63
Research and Administration	72
Strategic Operations.....	77
Student Life.....	79
Technology Transfer	84
University Advancement.....	87

Section 4 – Links to Key Laws and Regulations	89
Academic Affairs.....	89
Admissions.....	93
Athletics.....	94
Finance and Administration	95
Financial Aid.....	98
Graduate Studies	100
Human Resources	101
Information Technology.....	104
Plant Operations.....	106
Research and Administration	110
Strategic Operations.....	112
Student Life.....	112
Technology Transfer	114
University Advancement.....	115

Section 1 – Executive Summary

Overview

During the past 10 years, Colorado School of Mines (CSM) has undergone a transformation. It has evolved from a small, high-quality science and engineering college to a cutting edge research institution with a worldwide reputation and presence. In the last 10 years, CSM has experienced substantial growth in enrollment, research funding, and programs. The composition of the student body has also changed significantly. Specifically, since 2001:

- **Enrollment has increased by 65 percent over the past decade.** Graduate and undergraduate enrollment has increased from about 3,250 in the 2001-2002 academic year to about 5,350 in the 2011 fall semester.
- **Operating revenue has more than doubled - from \$63 million in Fiscal Year 2001 to \$139 million in Fiscal Year 2010.** Research expenditures have grown from around \$19 million in Fiscal Year 2001 to \$53 million in Fiscal Year 2011. Research dollars represented about 22 percent of CSM's total expenditures in Fiscal Year 2001 compared to an estimated 25 percent of total expenditures in Fiscal Year 2011.
- **Programs have expanded.** Faculty and staff alike comment not only on tremendous expansion in key academic areas such as physics and computer science, but also on new international initiatives and partnerships underway in Abu Dhabi, Brazil, and Indonesia. CSM is also a leader in providing continuing professional education to science and engineering professionals in private industry.
- **Composition of the student body has changed dramatically.** CSM has changed from a state-focused and primarily male-dominated institution, to an institution with a global and diverse population. The student body is now 25 percent female and over 10 percent of its students hail from countries outside the United States.

CSM's transformation presents both benefits and challenges. CSM's unique niche and international reputation now attract top research faculty, high-quality students, and an impressive list of industry partners. As noted above, despite the economic downturn, the School has experienced significant growth. Yet the current State fiscal crisis impacts CSM's ability to develop an infrastructure commensurate with increases in student enrollment and growth in research and academic programs. The current environment places a premium on prioritizing resources and mitigating potential risks.

The Report

This report presents the results of Two Hills Accounting & Consulting's review of compliance risks facing CSM, along with recommendations for improving the compliance infrastructure. The report is organized as follows:

Section 1 – Executive Summary. This section highlights (1) the purpose, scope and methodology of our review; (2) specific strengths CSM brings to the compliance environment; (3) institution-wide infrastructure issues and opportunities for establishing a strong compliance environment and program; (4) a summary of key compliance risks we identified in our interviews with compliance partners; and (5) an entity-wide heat map.

Section 2 – Key Risk Areas. The second section of the report provides a summary of key compliance risks faced by CSM, including laws and regulations and opportunities for mitigating risks.

Section 3 – Functional Areas. This section provides detailed compliance information on the functions and programs of the University. It includes a (1) listing of the compliance partners; (2) matrices that consist of an inventory of key compliance requirements affecting the operations in each area, ratings on the likelihood and impact of a compliance failure, and potential controls to mitigate compliance risk; and (3) compliance risk heat maps. The ratings in this section were determined through discussions with compliance partners, reviews of audits of CSM and other universities and our judgment.

Section 4 – Resources. This section includes highlights of laws and regulations, web links and tools to assist CSM with managing its compliance requirements and building a strong compliance program.

Purpose, Scope and Methodology

The purpose of our engagement was to develop an inventory of key compliance risks, craft a methodology that the School could use to conduct on-going assessments of compliance, and assess the likelihood and impact of potential compliance failures. To that end, we worked with executive management and internal audit to identify the functions and programs to be included in our review. Our review included:

- Academic Affairs
- Admissions
- Athletics
- Finance and Administration
- Financial Aid
- Graduate Studies
- Human Resources
- Information Technology

- Plant Operations
- Research and Administration
- Strategic Enterprises
- Student Life
- Technology Transfer
- University Advancement

For each of the functions and programs listed above, we worked with executive management and internal audit to identify a “compliance partner” who was knowledgeable or accountable for meeting compliance requirements for his or her area of responsibility. We interviewed each of these compliance partners, as well as CSM executive management and legal counsel. We did not conduct substantive tests of the effectiveness of compliance systems and controls. While not an exhaustive inventory, we identified key laws and regulations brought to our attention by compliance partners. Further, we caution that the volume and complexity of ever-changing laws and regulations merits continued on-going scrutiny. Our work was intended to form a foundation for a future compliance program that would examine critical compliance areas.

To develop our methodology, we reviewed compliance literature and compliance risk assessment information and tools prepared by the Association of College and University Auditors (ACUA) and higher education institutions, including the University of Minnesota, Texas A&M University and the California Institute of Technology. We developed a template of compliance requirements and recommended controls for the CSM functions and programs listed above. We interviewed compliance partners about the requirements contained in the template and asked them to verify the relevance of the requirements to CSM and to identify any other relevant compliance requirements not listed on the template. During our interviews, we asked each compliance partner to assess each compliance requirement in their area by rating: (1) the likelihood of a compliance failure for that requirement and (2) the impact to the institution if a failure occurred. We developed heat maps and updated compliance templates based on these scores. Heat maps and compliance templates for each CSM function or program reviewed are located in Section 3 of this report.

Finally, we analyzed interview data and compliance risk scores, as well as reviewed audits and compliance issues at other universities, to identify significant institution-wide issues and themes, including CSM’s compliance strengths, opportunities for improving compliance and CSM’s key compliance risks. We also collected resources and tools to assist CSM and its new compliance officer in building a strong compliance program.

Strengths CSM Brings to the Compliance Environment

During our review, we identified a number of strengths that indicate the School of Mines is well positioned to develop a strong compliance program. We highlight these strengths below.

Culture of Ethics and Integrity

A strong ethical culture is crucial to maintaining and expanding CSM's reputation as a premier science and research institution:

"Running an ethical company that places a high value on compliance is not just simply a good idea. It also makes good business sense. One hears all about the importance of business ethics, the damage that can be caused by scandals...But less is heard about how an ethical business with strong corporate governance will outperform companies that don't focus on ethics."

Martin T. Biegelman, "Building A World-Class Compliance Program"

In our interviews with over 30 compliance partners in CSM leadership positions, we consistently heard of a campus-wide commitment to the goals of the University; trust and respect for fellow students, faculty, and staff; and dedication to and passion for CSM's mission – all hallmarks of a world-class, ethical organization. Despite extraordinary demands, faculty and staff appear to be energized by their opportunities to build CSM into a global leader in energy, physics, and the earth sciences.

We also heard that the "tone at the top", the most critical element in developing an ethical organization, was outstanding. Compliance partners mentioned, for example, that the Board of Trustees and President have had a real impact in setting high standards and, despite challenges, obtaining the resources needed to develop an infrastructure that supports growth.

Development of a Highly Qualified and Dedicated Staff

We were impressed by the commitment of CSM to recruiting and hiring the best. Compliance partners told us that, although significant turnover in key positions has occurred in recent years, they were pleased with the experience and expertise of current leadership. For example, we were informed of significant positive changes in financial and grants administration over the last five years. This is supported by a review of CSM's audit findings – ten years ago the School faced continuing challenges in compiling annual financial statements in accordance with accounting standards and complying with laws, regulations and contract commitments. This year's audit is reportedly "clean;" financial staff is working on infrastructure and control improvements. This is not to say that challenges do not exist, but rather to observe that the current team has placed an emphasis on creating the proper systems and controls.

Opportunities for Improving the Compliance Infrastructure

We identified over-arching campus-wide infrastructure improvements that could strengthen the compliance control environment and support the institution's continued growth and expansion. We believe that committing to, and investing in, these infrastructure improvements could both streamline campus activities and reduce the costs associated with managing and carrying out compliance functions. Additionally, these improvements could better position CSM to develop cutting-edge research opportunities while enhancing the infrastructure needed to support and sustain a leadership role in the earth, energy and environmental fields. These infrastructure enhancements include:

Improving the Information Technology Infrastructure

During our interviews, information technology (IT) staff and compliance partners in other functional areas repeatedly spoke about CSM's significant institution-wide technology needs. Compliance partners consistently noted gaps between the institution's IT capabilities and CSM's need for leading-edge technological support. We learned of concerns about the lack of protection of proprietary research data on computing systems and of information on paper records and files vulnerable to theft or misuse. Compliance partners told us the School has a real opportunity to develop better research tools, enhance on-line training capabilities and improve the security of critical records. Indeed, all of the infrastructure needs and solutions identified in our review, discussed in the three sections that follow, require at least some level of IT support. While the current information technology team appears to be well informed on compliance issues and proactive in addressing risks, we were informed by multiple sources that IT demands far outstrip available resources.

An investment in IT infrastructure, including developing increased capability to automate processes and tools, is crucial to supporting and streamlining CSM's compliance activities and to sustaining CSM's mission. Although addressing IT needs within the current budget environment is not without challenges, we believe that prioritizing needs in this area will ultimately serve CSM well, particularly in promoting CSM's research capabilities and sustaining its reputation in the long term. Innovative approaches will be needed, including acquiring IT staffing, installing hardware and software systems, and considering short-term contract assistance to address critical project backlogs and needs.

Establishing a Compliance Accountability Structure

We asked compliance partners if they could identify those individuals responsible for ensuring compliance with various laws, regulations, and contractual provisions. Respondents could generally identify directors and faculty department heads responsible for certain requirements, but overall, could not confirm whether these individuals were responsible for training, monitoring or holding others accountable for compliance. More commonly, compliance responsibilities were shared among more than one individual. Further, certain requirements, such as those governing disclosure of personal information,

crossed more than one academic department or administrative unit. For these types of requirements, respondents could not identify who was responsible for overseeing and enforcing requirements. Further, we found that CSM has, for the most part, not required faculty, staff and student interns to periodically certify that they are aware of various compliance requirements, including conflicts of interest and responsibility for protecting student information.

Given the fact that compliance is quite often an “other duty” imposed on already overburdened faculty and staff, many colleges and universities have struggled with developing a cost effective compliance structure. For example, in 2007, according to its Associate Vice President for Compliance and Ethics, Georgetown University’s approach to compliance was in the process of changing from reactive and decentralized, to proactive and “systematic without centralized control or micromanagement.” Georgetown’s website currently identifies faculty and staff responsible for various compliance areas, offers web-based compliance tools and resources, and provides links to reporting compliance concerns. (<http://compliance.georgetown.edu/complianceaccountability/>)

To its credit, CSM’s leadership has taken a significant step in strengthening the compliance environment. The new Director of Compliance will provide leadership for establishing an operational framework for institutional compliance and, in partnership with operational units, develop compliance structures, reporting mechanisms, and systems.

Enhancing Training

CSM could significantly enhance its infrastructure by making improvements in compliance training offered to faculty, staff and student interns. Compliance partners consistently spoke about the need for training in key compliance areas, especially where the complexity and volume of requirements have spiraled – such as research administration and the management of grants and contracts. We were told the lack of training directly affects staff awareness of and compliance with complex laws and regulations. For example, faculty and student organizations may unwittingly enter into contracts or agreements that violate complex export control laws.

We were informed that, at present, various individuals decide when and how to provide training and that training records are neither maintained consistently nor centrally, such as through an automated online tracking mechanism. Many compliance-related trainings, including training associated with complex federal employment laws and grant requirements, are available in an online format. Compliance partners told us that other institutions make these mandatory and voluntary training resources available online; CSM may be able to acquire some of these online trainings inexpensively or partner with other institutions to obtain or modify existing training resources. Establishing a centralized accountability structure for identifying training needs, developing training resources, and maintaining training records is key to supporting and maintaining a strong compliance culture and function.

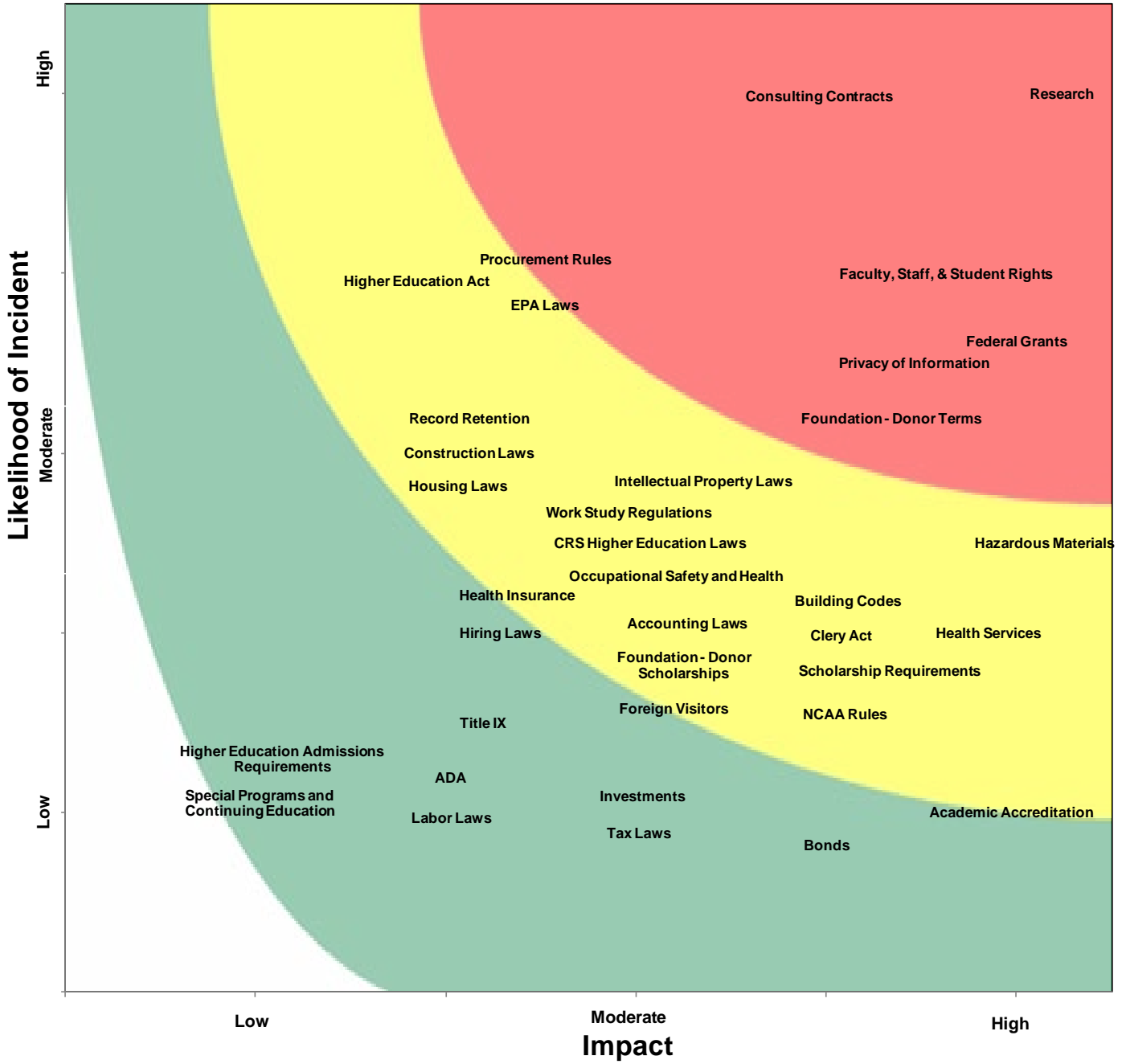
Developing a Repository for Reporting Requirements

CSM would benefit from developing a central repository for department reporting requirements and reports, especially since the volume and complexity of these requirements are continually increasing. The absence of a repository became clear when we asked compliance partners for lists of reports or reporting requirements for their areas of responsibility and found the lists were not readily available. Managing extensive reporting requirements is time consuming and, if overlooked, can be damaging to the institution. For example, audits of federal grants at universities often contain findings noting problems with failing to submit required reports or with submitting these reports in a timely manner. Generally, we believe most directors are aware of their reporting schedules. However, when staff members leave or new requirements come into play, staff may face a steep learning curve. Several compliance partners noted challenges with learning new reporting requirements under the Higher Education Act and the related Integrated Postsecondary Education Data System (IPEDS). Centralized online reporting systems, including regular notifications to remind those responsible for reporting requirements and deadlines, could help manage these requirements more efficiently and enhance oversight of deadlines.

Identification of Risk Areas

We rated the likelihood and impact of a compliance failure using feedback from campus-wide compliance partners combined with our knowledge and understanding of the experience of other colleges and universities. The results are displayed in the university-wide compliance risk heat map below. The items in the heat map reflect groups of laws, regulations, or contract provisions that would likely be addressed with a cohesive system or set of controls. We acknowledge that the results involve a high degree of judgment, and we underscore our hope that they form the foundation for an open and on-going dialogue on how to use scarce resources to best address key risks.

University-wide Compliance Risk Profile



As portrayed in the university wide heat map, we identified specific compliance requirements that, due to their importance to or potential impact on the institution, are high-risk and merit the attention of CSM's leadership. These include federal and state laws and regulations related to:

- **Research**, including laws and regulations governing export controls, human subject research and technology transfer.
- **Federal Grants**, including laws and regulations governing cost-allowability, time reporting, procurement, property management, codes of conduct (including conflicts of interest), audits and cost sharing arrangements.
- **Professional Consulting Contracts**, including laws and regulations governing ethics, confidential information, conflict of interest and private use of state property.
- **Donations**, including compliance with donor agreements.
- **Protecting the Rights of Faculty, Staff and Students**, including laws governing discrimination and sexual harassment.
- **Protection of personal information**, including laws governing educational records and privacy of information.

Section 2 – Key Risk Areas

Research

Currently CSM receives over \$50 million in sponsored research annually and has a goal to increase research revenue by about \$30 million over the next few years. Many of the research activities associated with CSM's grants are subject to a complex body of federal and state laws and regulations. Violations of some of these laws could result in significant financial penalties and damage to CSM's reputation. Examples of some of the major federal laws impacting research activities at higher education institutions include:

Export Control Laws. Export control laws are federal laws and regulations intended to restrict export of goods and technology that could contribute to the military potential of adversaries, prevent proliferation of weapons of mass destruction (nuclear, biological, chemical) and terrorism, and enforce trade agreements and sanctions against other nations. Export control laws may require an individual to obtain a government license before sending or taking certain equipment, chemicals, or technologies outside the U.S. Additionally, these laws may prohibit foreign researchers or students from participating in research involving equipment, chemicals, or technologies subject to export control laws. Penalties for violating export control laws are severe. Individuals and institutions may be subject to civil and criminal penalties amounting to millions of dollars; individuals found criminally liable may also be incarcerated.

Human Subjects Research. The U.S. Department of Health and Human Services, Office for Human Research Protections, has promulgated regulations to ensure the ethical practice of research involving human subjects. Research sponsored by other federal agencies and private industry may have additional requirements for human subjects research. Human subjects research regulations are complex and if violations occur, institutions may be subject to a range of penalties, including temporary withholding of payment, repayment of funding, or suspension or disbarment, which disqualifies the institution from receiving federally sponsored grants.

Research Misconduct. Research misconduct is defined as plagiarism; fabrication or intentional falsification of data, research procedures or data analysis; or other deliberate misrepresentation in proposing, conducting, reporting or reviewing research. It does not include honest error or honest differences in interpretations or judgments of data. In general, institutions are responsible for fostering a research environment that promotes the responsible conduct of research, discourages research misconduct, and responds promptly to allegations or evidence of possible research misconduct. Findings of research misconduct for federal-funded research grants may result in a range of penalties, including letters of reprimand, suspension or disbarment and recovery of federal funds.

Technology Transfer. Under the Bayh-Dole Act of 1980, higher education institutions have responsibility for promoting the transfer of their research results to the commercial marketplace for the public benefit. Under the Act, institutions retain ownership to

inventions resulting from federally-funded research. In return, universities are expected to file for patent protection and to ensure commercialization upon licensing. The royalties from such ventures are shared with the inventors, the institution and department sponsoring the research, and the technology transfer process. Institutions must report the results of their technology transfer efforts to the federal funding agency annually.

What We Learned

Our interviews revealed widespread concerns among compliance partners regarding the complexity of laws and regulations governing research compliance. Compliance partners were concerned that faculty members are unaware of when complex compliance requirements, such as export control laws or human subject research, apply. Compliance partners were also concerned about the lack of adequate, centralized infrastructure for supporting the growth of the research function at CSM. Examples of some of the concerns specifically noted by compliance partners were:

- **Export Controls.** Compliance partners raised concerns about whether CSM had identified all excluded software technologies and ensured that all international students who should be excluded from these technologies had been identified. Some partners noted that a graduate student could potentially bring an international student into a laboratory with excluded technology during off hours without detection. Partners also raised concerns about international research efforts and whether these efforts had received adequate scrutiny to ensure export control laws were not implicated. Concerns were also raised about whether faculty members were ensuring that laptops and thumb drives were wiped clean before traveling internationally.
- **Human Subjects Research.** Compliance partners noted that, although CSM does not have the volume of human subjects research experienced at institutions with medical schools, CSM activities that could trigger human subjects research requirements have increased. More than one compliance partner mentioned an increase in pedagogical surveys and noted that some of these surveys may qualify as human subjects research. Partners raised concerns about whether faculty were adequately aware of when human subjects research requirements might be implicated so that appropriate review could occur.
- **Research quality and performance.** Although compliance partners generally believed that research was of consistent high quality at CSM, some partners did raise concerns about the adequacy of research performance monitoring. Compliance partners noted that isolated problems with research performance, which have occurred in the past, could impact not only the reputation of the principal investigator, but could also have a negative impact on CSM's reputation. Serious issues with research quality may also impact the availability of future research funds from the research sponsor.

How the Risk of Noncompliance Could Be Mitigated

Compliance Partners made a number of suggestions for improving oversight of research compliance. In particular, compliance partners commented on a need for additional:

- **Training.** Compliance partners identified a need for regular and systematic training, including online training. We identified other large research institutions with comprehensive online research compliance training materials and curricula (e.g., University of Kentucky); CSM could potentially use these institutions as models and scale the curricula and online training materials to meet CSM's specific requirements.
- **Centralized infrastructure and accountability.** Compliance partners noted that clear lines of accountability for research compliance requirements, such as export control laws, human subjects research, and research performance, were generally lacking at CSM. Currently CSM is working on a new position that would handle export control laws and human subject research as part of its job responsibilities; this is a positive step. However, clearly assigning lines of accountability for all compliance requirements and communicating the accountability structure institution-wide would help provide a better infrastructure for CSM's growing research efforts.
- **Automated resources and tools.** An investment in automated resources and decision tools would also enhance the infrastructure for supporting research compliance. Compliance partners commented that many of the processes supporting research compliance are manual. Automated decision tools could be used to assist with evaluating complex research requirements, such as export control laws, to specific research efforts. Centralizing research regulations, supporting documents, institutional policies and training materials on one website could provide a one-stop shop to assist researchers with resolving questions about compliance issues.

Finally, because of the importance of research to both CSM's revenue and reputation, it may be prudent to invest resources in ongoing monitoring of research compliance.

Federal Grants

Research grants and contracts are essential to achieving CSM's global academic and research objectives. As noted previously, funding in this area has increased dramatically over the past decade, from about \$19 million in 2001 to \$53 million in 2011, an increase of about 65 percent. While the growth is surprising given the current economic climate, it is reflective of the School's commitment to increase its focus and national role as a research institution. Federal grant revenue comprises over 60 percent of total grant and contract funding. In general, federal grants must be audited annually. The importance of

compliance with federal grant requirements cannot be overstated. “A Primer on Avoiding Grants Management Minefields” (Jill Mortali and Sarah T. Axelrod, Harvard, Spring 2007) emphasized the importance of strong compliance controls, noting questioned costs and settlements in the millions. The authors specifically highlighted cost allowability issues (University of Minnesota - \$32 million); effort certification weaknesses (Northwestern University - \$5 million, Johns Hopkins University - \$2.7 million); and research compliance (Cornell University - \$4.4 million). A complex set of laws, regulations, and grant terms and conditions, govern the expenditure of federal funds. Of particular importance and relevance to institutions of higher education are the following:

Office of Management and Budget (OMB) Circular A-110: “Uniform Administrative Requirements for Grants and Agreements with Institutions of Higher Education, Hospitals, and Other Non-Profit Organizations.” Circular A-110, for example, addresses critical compliance areas such as reporting, procurement, property management, codes of conduct (including conflicts of interest), audits and cost sharing arrangements.

Office of Management and Budget (OMB) Circular A-21: “Cost Principles for Educational Institutions.” A voluminous and highly complex directive, Circular A-21 sets forth specific compliance requirements for allowable costs, including guidance on 54 selected cost items (training, travel, rent, salaries, meetings, conferences, entertainment, compensation for personal services, etc.).

Other OMB Guidance: Circular A-133 sets forth standards for obtaining consistency and uniformity among federal agencies for the audit of non-federal entities expending Federal awards, including sub-recipient monitoring. Other circulars and laws (Circular A-129 and the Cash Management Act) describe requirements for managing cash drawdowns and ensuring non-delinquency.

Specific Grant Terms and Conditions: Federal agreements generally contain specific requirements related to accomplishing the objectives of the grant and the deliverables, along with boilerplate language for compliance with over-arching federal laws and regulations, such as laws governing for example, environmental protection, historic preservation, and civil rights.

Material noncompliance with federal laws, regulations, and the terms and conditions of grants, typically identified through audits, investigations and monitoring reports, can result in federal agencies withholding cash payments, disallowing costs, suspending or terminating a specific award, withholding further awards, or applying other civil or criminal remedies. In addition to any penalties imposed by the federal government, there are notable examples of damage to the reputation of agencies and institutions for noncompliance.

What We Learned

In general, compliance partners told us that CSM has significantly improved awareness of federal requirements and systems and procedures supporting compliance, thus mitigating risk in this area. Further, we were informed that the School has recently had fairly “clean” audits. However, the amount of federal funding received by CSM, the complexity of the laws and regulations governing use of federal funds, the limited resources available for training and for monitoring expenditures, the annual audit requirements, and our analysis of audit findings at universities throughout the nation suggest continued focus on the area.

For example, both faculty and staff noted opportunities to improve practices regarding time and effort reporting and certification, commenting that CSM had a “wake-up” call several years ago. Those we interviewed noted that although practices had changed and enforcement stepped up, opportunities for improvement remain. For example, faculty attest to the accuracy of time spent on federal projects, but may not have the information to verify reports because research assistants do not fill out time cards and may not be co-located. In addition, the frequency of certification may not be optimal – reportedly once a semester versus monthly or biweekly. We also learned that CSM needed to conduct the required independent internal evaluation of compensation for personal services charged to sponsored agreements, but had not yet done so.

How the Risk of Noncompliance Could Be Mitigated

Training. Compliance partners consistently reported the need for training in a wide variety of subjects, including federal grants. Given the volume, complexity and ever-changing nature of laws and regulations in this area, we believe enhancing training is warranted. Training could initially be focused on key compliance risks. The above-referenced Harvard compliance study flagged 10 “hot topics” – requirements frequently the subject of audit findings. These include effort reporting; over-commitment of principal investigator and key personnel effort; sub-recipient monitoring; cost transfers; allowable direct charges (in particular “sensitive costs such as administrative and clerical salaries, general purpose equipment, software, office supplies, memberships, alcohol and entertainment); allocability; cost sharing; travel; and accelerated spending. From our experience and review of prior audits of CSM and other universities, these “hot topics” are well worth the focused attention of management.

Oversight. Resource constraints make oversight and enforcement difficult. However, given the growth in federal grants, ensuring that those responsible for administering particular grants closely monitor compliance could help mitigate risks.

Professional Consulting Contracts

CSM policies authorize faculty to engage in professional consulting and recognize that consulting activities can foster professional growth and lead to the development of potentially valuable external contacts for CSM. Accordingly, faculty and staff may enter into professional consulting agreements with external entities, such as private industry or other institutions of higher education. CSM policies require approval of professional consulting agreements by the department head in advance of execution.

CSM policies governing professional consulting contracts reflect a body of state laws and executive orders addressing ethics, confidential information, conflict of interest and private use of state property. In accordance with these laws, CSM employees are prohibited from disclosure or use of confidential information acquired in the course of official duties for personal financial benefit and from acceptance of any substantial economic benefit as a reward or inducement for improper discharge of public duties. CSM employees are also prohibited from acquiring or holding an interest, directly or indirectly, in any business or undertaking that may be economically benefited by their work at CSM and are required to disclose conflicts of interest. CSM employees are also prohibited from using CSM property, equipment, or supplies for private gain. Policies also prohibit employees from using CSM's name or logo in connection with private activities and from intimating that CSM has sanctioned any personal undertaking.

A strong commitment to ethical conduct by CSM's faculty and staff is crucial to the School's long-term financial sustainability and reputation. The public has a low tolerance for questionable ethical behavior by public officials, employees, and institutions. Issues of questionable ethical conduct, if surfaced, could affect donor contributions and funding by federal and private industry sponsors.

What We Learned

During our interviews, compliance partners consistently raised concerns regarding oversight of professional consulting contracts. In particular, compliance partners were concerned that faculty members were entering into consulting contracts without obtaining CSM approval in advance, a violation of School policy. Compliance partners also noted that good mechanisms were needed to "police" professional consulting contract disclosures and approvals. In addition, compliance partners identified the following issues related to professional consulting contracts:

- **Non-disclosure agreements.** Compliance partners were concerned that faculty and graduate students were signing non-disclosure agreements as part of their contracts with private industry without obtaining legal advice or review. A non-disclosure agreement could prohibit faculty and students from publishing the research results performed as part of the consulting contract, impairing the benefit of the research to the public. Research for public benefit is a focus of CSM specifically and of public institutions of higher education in general.

- **Conflict of interest disclosures.** Compliance partners reported that current mechanisms for reporting and disclosing conflicts of interest were not adequate. Partners mentioned that a conflict of interest disclosure form was being revised and a conflicts committee would soon be activated to review disclosures. Compliance partners were concerned that faculty could be entering into professional consulting agreements with entities or forming equity interests with organizations that had an existing relationship with CSM, a violation of state law and CSM policy.
- **Using public resources for private benefit.** Compliance partners were concerned that faculty may be using CSM resources, such as laboratories and equipment, to perform work on their professional consulting contracts without reimbursing CSM for the use of these resources, a violation of State law and CSM policy. Compliance partners also raised concerns about CSM inadvertently becoming a party to a professional consulting agreement. This could occur when the research sponsor believes the agreement is between the sponsor and CSM rather than between the sponsor and an individual faculty member. By accepting payment made by the research sponsor to CSM, CSM may become obligated for performance on the contract.

How the Risk of Noncompliance Could Be Mitigated

Conducting ongoing training and education. CSM’s policies on professional consulting contracts, conflict of interest disclosures, confidentiality and private use of School resources need to be regularly communicated and emphasized through training on a regular and ongoing basis. Case study training that helps faculty and staff negotiate particularly complex and “real life” situations encountered routinely at CSM could be especially beneficial.

Adopting annual conflict of interest disclosures and certifications. CSM could adopt an annual conflict of interest disclosure process for all faculty and staff. Annual conflict of interest disclosures are routine in many organizations with high public scrutiny and access to sensitive information. CSM could further enhance the annual disclosure process by asking faculty and staff to certify their understanding of and compliance with state laws and School policies governing professional consulting agreements, conflict of interest disclosures, and private use of public property.

Maintaining a central repository of professional consulting and nondisclosure agreements. Currently CSM administration is not aware of the volume of professional consulting agreements executed by faculty and staff. Once disclosed, maintaining a central repository could aid in monitoring these agreements and managing potential conflicts that may arise as a result of these agreements. CSM administration could then update or revise any policies, as indicated, by regular monitoring of these agreements.

University Advancement

The School of Mines Foundation, an independent tax-exempt entity founded in 1928 and incorporated in 1951, is the official gift-receiving agency for the institution. The Foundation has played a pivotal role in maximizing private sector support for the School. Donors have the option of contributing either restricted or unrestricted gifts. Unrestricted gifts provide financial support for on-going, day-to-day operations, including scholarships; whereas restricted support is designated for particular purposes, including funding faculty chairs, professorships and support for specified research endeavors. The Foundation held an endowment for the School of \$196 million as of June 30, 2011 and provided about \$10 million in revenue during Fiscal Year 2011.

Compliance with the terms and conditions of restricted donations is critical for ensuring the trust and confidence of donors and ultimately, the continued support of the School. Likewise, ensuring unrestricted funds are spent wisely is important to promoting philanthropic giving. In a well-publicized case, the reputation of the University of Colorado and its Foundation was jeopardized because of audit findings regarding the lack of a clear, coordinated system for meeting donor intent. The 2005 audit cited inadequate documentation and poor coordination between the Foundation and the University; the lack of regular audits of the use of donations; commingled accounts; and improper use of funds including food and catering, alcohol, flowers, gifts, and limousine services. The University of Colorado, recognizing the reputational damage potential, moved quickly to improve systems and controls.

What We Learned

The School's fund managers in various departments throughout the campus oversee more than 1,000 donor accounts. The volume of accounts and transactions combined with the decentralized nature of the spending and the importance of stewardship to gift giving, make reducing risks in this area important.

Compliance partners told us that, while they are generally comfortable with the propriety of restricted and unrestricted expenditures, improvements in accounting systems and controls are needed. We were informed that although significant progress has been made in the last six months, recommendations contained in a 2009 internal audit report on the use of Foundation funds have not yet been fully implemented.

While not specifically compliance related, another risk worthy of note came to our attention. We were informed of potential missed opportunities to increase philanthropy and develop the donor base. In particular, stronger ties between the Foundation and the School and forging partnerships between faculty and Foundation staff would enable fundraisers to identify compelling needs and better share the impact of gift giving.

How the Risk of Noncompliance Could Be Mitigated

Compliance partners made a number of suggestions for mitigating the risk of noncompliance, all in line with the 2009 internal audit. These include:

Timely and Complete Financial Activity Reports at the Fund Administrator Level:

Monthly reports containing a list of accounts by fund administrator and information on account status (beginning balances, expenditures, and ending balances) would help department heads and administrative assistants better monitor donor accounts. We were informed that CSM staff is currently working on improving financial information available to fund administrators.

Fund Manager Certification: CSM could strengthen controls over expenditure of donated funds by implementing a recommendation in the 2009 internal audit requiring fund administrators to certify that monies have been properly spent. Certification is important to focus attention on the responsibility and accountability for managing donated funds and to ensure expenditures are periodically reviewed.

Training: Compliance partners told us that fund administrators need more training on how to access electronic donor account information. We were informed that more in-depth, hands-on training on the Banner System, for example, would help department heads and administrative assistants better monitor accounts.

Protecting the Rights of Faculty, Staff and Students

With over 800 faculty and staff, including scholars, research and finance professionals, information technology professionals, labor and trades workers, administrative assistants, athletics and student life professionals, the School of Mines has far-reaching responsibilities under federal and state laws and regulations. In addition, the School oversees a diverse, international student body of over 5,300. The EthicsPoint reporting system recently adopted by the School provides a summary of risk categories in the human resources area, including discrimination/harassment; Equal Employment Opportunity Commission or Americans with Disabilities Act matters; employee misconduct; sexual harassment; and conflict of interest, among others.

Notably, at Mines as at other universities, legal resources are often focused on human resource issues. Failure to ensure a safe environment and fair and equitable treatment can increase financial and reputational risk. The publicity surrounding high profile cases, the drain on faculty and staff, and ultimately the costs of litigation and settlements can cause irreparable damage. The lengthy battle over allegations that the University of Colorado violated Title IX provisions, fostering an atmosphere hostile to women in its football program, has had ripple effects throughout the nation. Lafayette College, a small institution in the East recently settled a \$1 million lawsuit brought by five women against a public safety officer. This year, Yale students filed suit under Title IX alleging “failure to address

incidents of sexual harassment and sexual assault has created a ‘hostile environment.’” In June 2010 the Departments of Justice and Education issued a joint letter discussing concern about the use of “electronic book readers that are not accessible to students who are blind or have low vision”, the subject of a National Federation of the Blind complaint against Penn State. In short, whether plaintiffs prevail or whether governmental immunity protects state institutions, every challenge comes at a cost.

There is a large and complicated body of laws and regulations governing various aspects of the School’s human resource administration. The Equal Employment Opportunity Commission (E.E.O.C.) website notes the following:

- Title VII of the Civil Rights Act of 1964 makes it illegal to discriminate against someone on the basis of race, color, religion, national origin, or sex and prohibits retaliation. The law also requires employers to reasonably accommodate applicants' and employees' sincerely held religious practices, unless doing so would impose an undue hardship on the operation of the employer's business. Sexual harassment, often the subject of allegations, is illegal according to the E.E.O.C. when it is so frequent or severe that it creates a hostile or offensive work environment or when it results in an adverse employment decision (such as the victim being fired or demoted). The harasser can be the victim's supervisor, a supervisor in another area, a co-worker, or someone who is not an employee of the employer, such as a client or customer.
- Title IX of the Education Amendments of 1972 prohibits discrimination on the basis of sex, requiring that "no person in the United States shall, on the basis of sex, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any education program or activity receiving Federal financial assistance." Title IX has broad applicability.
- Other laws affecting protection of rights include the Equal Pay Act, Age Discrimination in Employment Act, and Americans with Disabilities Act.

What We Learned

The School of Mines, like any large institution, has significant challenges in ensuring a workplace and educational environment free from any type of discrimination or harassment. Allegations and legal challenges drain resources, and despite periodic in-class sexual harassment training, the School reportedly continues to have a number of harassment cases annually and receives reports of inappropriate faculty interactions with students.

Compliance partners noted that as a complement to the in-class sexual harassment training provided by Human Resources, the School would benefit from mandatory on-line training on a wide variety of employment and human resource topics. In addition, we learned that the School has neither an ombudsman nor an equity and diversity officer and only recently

obtained funding for a hotline complaint system - all of which are helpful in identifying and resolving issues before they are elevated.

How the Risk of Non-Compliance Could Be Mitigated

The School of Mines, like similarly positioned universities, has significant challenges ensuring compliance with laws in this area. The School has developed discrimination and sexual harassment policies and complaint procedures, along with enforcement mechanisms. However, compliance partners told us that although not a panacea, more in-class and on-line mandatory training could help. In addition, the new hotline will open up a reporting avenue that should allow CSM to more quickly respond to incidents and to aggregate useful information on problems identified.

Protection of Personally Identifiable Information

Broadly speaking, personally identifiable information (PII) is any information that can be used to distinguish or trace an individual's identity, such as their name, social security number, or biometric records. PII also includes information which, when combined with other personal or identifying information, can be linked to a specific individual, such as date and place of birth or mother's maiden name. A large body of federal and state law exists to protect the privacy of PII. Of particular importance and relevance to institutions of higher education are the following:

Educational Records under the Family Educational Rights and Privacy Act (FERPA) – FERPA protects against the disclosure of certain personally identifiable information contained in a student's educational record and applies to institutions that receive funding from the Department of Education. Violations of FERPA can result in the loss of federal funds, including federal financial aid.

The Privacy Act of 1974. The Privacy Act protects personally identifiable information by limiting the data that may be stored by a governmental agency and specifies that there must be appropriate technical and physical safeguards. Violations of the Privacy Act may result in civil fines.

Protected Health Information under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper or oral. Covered entities, such as CSM's health clinics, health plans and mental health clinics, may not disclose protected health information without the individual's written authorization. Non-willful violations of HIPAA may subject the institution to civil financial penalties; willful violations may subject an entity to both civil and criminal penalties.

Unauthorized disclosure of PII could be costly to CSM. In addition to the financial penalties noted above, CSM could incur significant costs for required notifications to victims affected

by information breaches and in some instances, could be subject to legal action. Further, the publicity associated with an unauthorized disclosure of PII by CSM could have a negative and costly impact to the institutions' reputation.

What We Learned

Our interviews with compliance partners identified a number of concerns with the protection of PII at CSM. Examples of some of the concerns specifically noted by compliance partners were:

- **Unencrypted electronic devices.** Compliance partners noted several areas where students' protected information is stored on unencrypted electronic devices, such as a laptop, thumb drive or mobile phone, increasing the risk of disclosure if the devices were lost or stolen. For example, admissions recruiters take unencrypted laptops with access to students' protected information off-site to recruiting locations and athletics staff members take laptops containing student athletes' grade point averages, class attendance records and health information to games. Compliance partners also reported that some faculty members maintain students' protected information on their laptops, thumb drives or phones and that these devices are not encrypted.
- **Hard copy records.** Compliance partners also raised concerns about adequate protection of hard copy records and files containing student personal information. For example, hard copy files containing personally identifiable information are left on workers' desks in the admissions area while in process and may not always be locked up at night. These files could be accessed by custodial staff or by a visitor to the admissions or registrar's area; no security system limits access to these areas during daytime hours. Some faculty post grades alphabetically, which may allow students to identify the grades received by their peers, a violation of FERPA. Finally, faculty members sometimes leave examinations out in the open, where students and others may be able to view the results, which is also a violation of FERPA.

How the Risk of Non-Compliance Could Be Mitigated

Since PII is widely available across campus, CSM needs a comprehensive mechanism to identify, classify, and safeguard its PII. If the institution is not aware of the PII and where it is located, it cannot develop a system to provide adequate protection. The National Institute of Standards and Technology's (NIST) April 2010 *Guide to Protecting the Confidentiality of Personally Identifiable Information* could provide CSM with a framework for this purpose. The *Guide* recommends that agencies (1) identify all PII residing in its environment; (2) minimize the collection, use, and retention of PII to only that information needed to meet its business needs; (3) categorize the confidentiality of the PII by impact level (low, medium, high); and (4) implement appropriate safeguards based on the PII impact level. Appropriate safeguards could include:

Strengthening Policies and Procedures. CSM should consider reviewing and revising policies for protecting PII using the NIST framework outlined above. In addition, policies should be disseminated regularly and posted in a centralized online location that can be readily accessed by all faculty and staff.

Conducting Training. CSM should consider ensuring all student and staff employees receive appropriate training before being granted access to automated or hard copy systems containing PII. Compliance partners consistently reported that more PII training needed to be provided and that it needed to be available on an ongoing basis. For example, compliance partners reported that student workers with access to PII do not consistently receive training on requirements for maintaining privacy. Additionally, staff may not be aware of HIPAA privacy requirements when students share information about their mental health or physical health concerns. An individual should be assigned accountability for maintaining training records; an online tool could streamline this process. Additionally, PII training could be provided online to reduce the need for classroom resources.

Implementing Access Control for Mobile Devices. CSM should consider ways to better secure PII maintained on portable and mobile devices, such as laptops and cell phones. The University could require full encryption of data maintained on mobile devices.

Monitoring and Enforcing PII Policies. CSM could implement monitoring software to track access and extraction of PII by faculty and staff. Supervisors and department heads should be trained to monitor their staff and enforce compliance with PII policies.

De-Identifying PII. Some staff may not need access to the full PII record to perform their job duties. For example, staff may not need access to the full record to examine correlations or trends used to support management and decision-making. CSM may want to consider options for de-identifying records when used for this purpose, so that the information remaining in the records does not identify an individual.

Section 3 – Functional Areas/ Compliance Partners

Academic Affairs:	Terence Parker, Provost/Executive VP Tom Furtak, Department Head, Physics Anthony Dean, Professor Lara Medley, Registrar
Admissions:	Bruce Goetz, Director of Admissions Heather Boyd, Director Enrollment Management Brandon Samter, Director International Student Services
Athletics:	Tom Spicer, Director of Athletics Brandon Leimbach, Associate Director Athletics
Finance and Administration:	Joe Trubacz, Senior Vice President for Finance and Administration Roger Cusworth, Controller Vicki Nichol, Director of Business Operations Kirsten Volpi, Former Vice President for Finance and Administration
Financial Aid:	Jill Robertson, Financial Aid Director
Graduate Studies:	Tom Boyd, Dean, Graduate Studies
Human Resources:	Michael Dougherty, Associate VP Human Resources
Information Technology:	Derek Wilson, Chief Information Officer Phil Romig III, Director Computing and Networking David Lee, Director, Enterprise Systems

Legal Counsel: Anne Walker, General Counsel
Esther Henry, Associate General Counsel

Plant Operations: Gary Bowersock, Director Facilities Management
Tim Sweitzer, Director Environmental Health and Safety
Linn Havelick, Director Environmental Programs (CSMRI)

President's Office: Bill Scoggins, President
Peter Han, Chief of Staff/Acting Vice President for Finance and Administration
Maureen Durkin, Director of Policy and Planning

Research and Administration: Ralph Brown, Director Research Administration

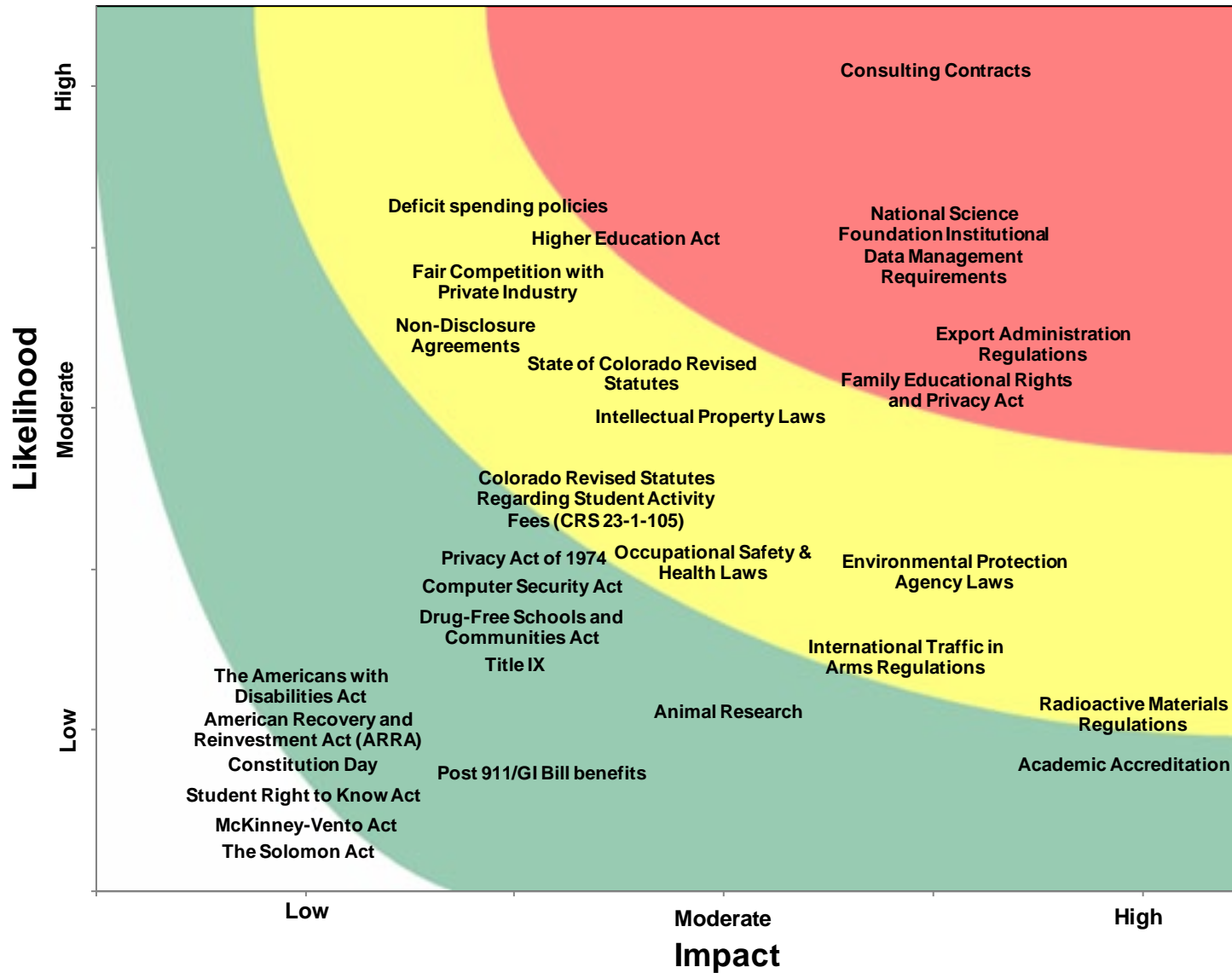
Strategic Enterprises: Nigel Middleton, Senior Vice President for Strategic Enterprises

Student Life: Dan Fox, Vice President Student Life
George Hughes, Public Safety Director
Lisa Goberis, Associate Director of Auxiliary Service
Ron Brummett, Director Student Services

Technology Transfer: John Poate, Vice President Research & Technology Transfer
Phil Romig Jr., Associate Vice President Research & Technology Transfer
Will Vaughan, Director Technology Transfer

University Advancement: Brian Winkelbauer, Executive Vice President University Advancement
Linda Landrum, Executive Vice President of Finance & Administration and
Executive Director
Rebecca Leewaye, Controller and Assistant Treasurer

ACADEMIC AFFAIRS



ACADEMIC AFFAIRS

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
Intellectual Property Laws	3	3	Training and awareness program
Properly license IP used by the university in profit generating engagements			Knowledgeable research staff who are aware of copyright issues
Properly license software			Corporate IP policy which is enforced in all areas
			Auditing of software
Export Administration Regulations	3.5	4.5	Have a research compliance officer perform reviews of activity, protocols, etc.
Export Control Laws			Establish export control compliance person
Data traveling out of the country			Implement an approval process for exporting items
International students viewing unauthorized data			
International Traffic in Arms Regulations	1.5	4	Have a research compliance officer perform reviews of activity, protocols, etc.
			Establish export control compliance person
			Implement an approval process for exporting items
Non-Disclosure Agreements	3	2	Legal counsel review
			Training and awareness program
Consulting Contracts	5	4	Legal counsel review
Arrangements /contracts reviewed for legal aspects and conflict of interest with the commercialization of technology (e.g. equity in start-up companies)			
Family Educational Rights and Privacy Act	3	4	Management oversight
Satellite systems holding data			Standardized student record keeping

ACADEMIC AFFAIRS

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
Faculty access to student data			Documented policies and procedures
Student pictures posted in departments			
Graded tests left in public areas			
Faculty release of student records to 3rd parties (surveys)			
Foundation access to student data			
Colorado Revised Statutes Regarding Student Activity Fees (CRS 23-1-105)	2.5	2.5	Documented policies and procedures
Use of student fees must follow laws and regulations and should not create liabilities for the school			Accurate accounting reports
			Periodic reconciliations
			Segregation of duties
			Training and awareness program
			Supervisory review and approval of reconciliations
Academic Accreditation	1	5	Documented policies and procedures
			Management oversight
			Designate an official to be responsible for leading accreditation efforts
			Develop a team of individuals to prepare for an accreditation review
			Training and awareness program
			University officials involved in process and attend accreditation meetings
American Recovery and Reinvestment Act (ARRA)	1	1	Management oversight

ACADEMIC AFFAIRS

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
Requirements for university reporting on vendors receiving ARRA funds			Review of sub-contractors
			Training and awareness
Occupational Safety & Health Laws	2	3	Training and awareness
Follow safety procedures for lab use			Provide appropriate laser glasses
			Install hallway warning signs
Environmental Protection Agency Laws	2	4	Training and awareness
Account for proper disposal of chemicals			Regular accounting for materials
Radioactive Materials Regulations	1	5	Special radiation safety training
Abide by state and federal radioactive materials handling laws and regulations			
National Science Foundation Institutional Data Management Requirements	4	4	Training and awareness
Proper protection on federal research data			Hardware security
Federal Grants	3.5	5	Regular transaction review
Proper cash handling	1	3	Independent review of expenditures
Deficit spending policies	4	1.5	Training and awareness
Proper expenditures	2	2	Provide accurate and timely accounting
Travel documentation	1	2	
Time and effort tracking	5	5	
Grant Closeout	2	4	
Freedom of Information Act (FOIA)	2	2	Monitoring
			Training and Awareness Program
			Documented policies & procedures
Colorado Open Records Act (CORA)	2	2	Monitoring
			Training and Awareness Program

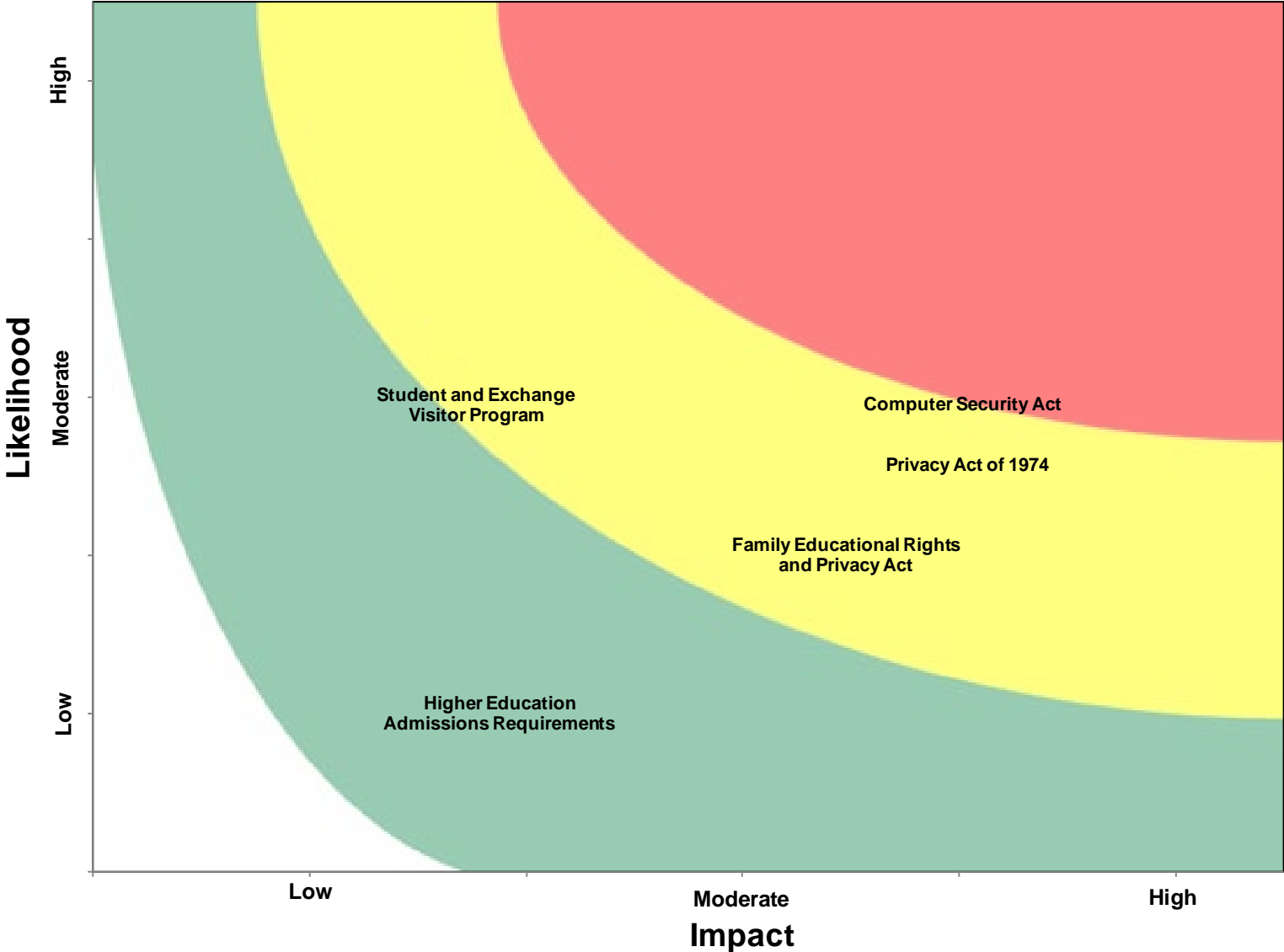
ACADEMIC AFFAIRS

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
			Documented policies & procedures
Human Subject Research	3	4	Training and awareness
			Establish Institutional Review Board
Animal Research	1	3	Research compliance office reviews
Review by animal care and use committee			IACUC reviews
			Inspections of facilities
			Training and awareness program
Drug-Free Schools and Communities Act	2	2	Documented policies & procedures
Privacy Act of 1974	2	2	Documented policies and procedures
			Tone at the top
			Training and awareness program
Computer Security Act	2	2	Documented policies and procedures
			Tone at the top
			Training and awareness program
Post 911/GI Bill benefits	1	2	Monitoring
			Training and Awareness Program
			Documented policies & procedures
The Americans with Disabilities Act	1	1	Protocol in place
			Procedures under review at Legal Services
			Once final, promulgate and distribute
			Essential function analyses completed on most jobs with physical demands

ACADEMIC AFFAIRS

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
			Post offer, pre-employment functional capacity evaluations obtained for those in jobs with physical demands
Constitution Day	1	0.5	Designated responsible party
			Documented policies & procedures
Student Right to Know Act	1	1	Documented policies & procedures
			Documented policies & procedures
Higher Education Act	4	2	Training and awareness program
Document a Missing Student Policy			Documented policies & procedures
Posting of Transfer Policies			Management oversight and review
Make the Cost of Textbooks Publicly Available			
State of Colorado Revised Statutes	3	2	Management oversight and review
Resident/Non-Resident Tuition Laws			Documented policies & procedures
CCHE Reporting Requirements			
Verification of Selective Service Registration			
Health Insurance/Immunization Requirements			
The Solomon Act	1	1	Documented policies & procedures
McKinney-Vento Act	1	1	Documented policies & procedures
Title IX	1.5	2	Documented policies and procedures
Gender Equality in Course Offerings			Training and awareness program
Student Right to Know Act			Compliance program/staff
			Compliance "tone from the top"
			Strategic plan
Fair Competition with Private Industry	4	2	Documented policies and procedures
			Centralized process for fee-for-service
			Management oversight and review

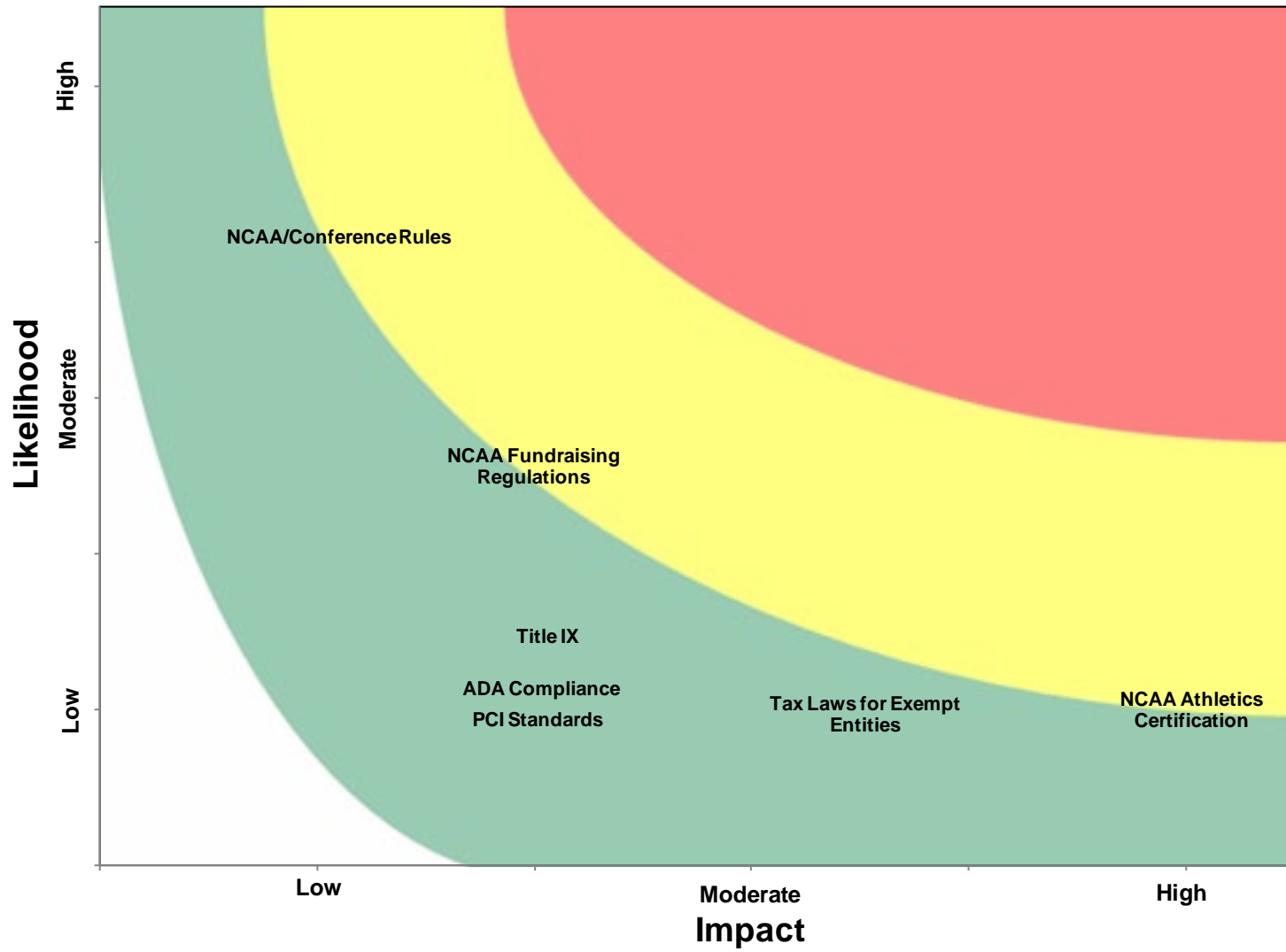
ADMISSIONS



ADMISSIONS

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
Family Educational Rights and Privacy Act	2	3.5	Documented policies and procedures
			Periodic automatic vulnerability scans of systems, networks, and devices
			Safeguarded storage for electronic data
			Provide FERPA training
			Store hard copy data in secured locations and shred data when no longer needed
			Training and awareness program
Privacy Act of 1974	2.5	4	Documented policies and procedures
			Tone at the top
			Training and awareness program
Computer Security Act	3	4	Documented policies and procedures
			Tone at the top
			Training and awareness program
Student and Exchange Visitor Program	2	3	Documented policies and procedures
Foreign student laws			Management review
VISAs			Training and awareness program
Higher Education Admissions Requirements	1	2	Documented policies and procedures
Resident/Non-resident enrollment ratio			Training and awareness program
Minimum student index			Management review

ATHLETICS



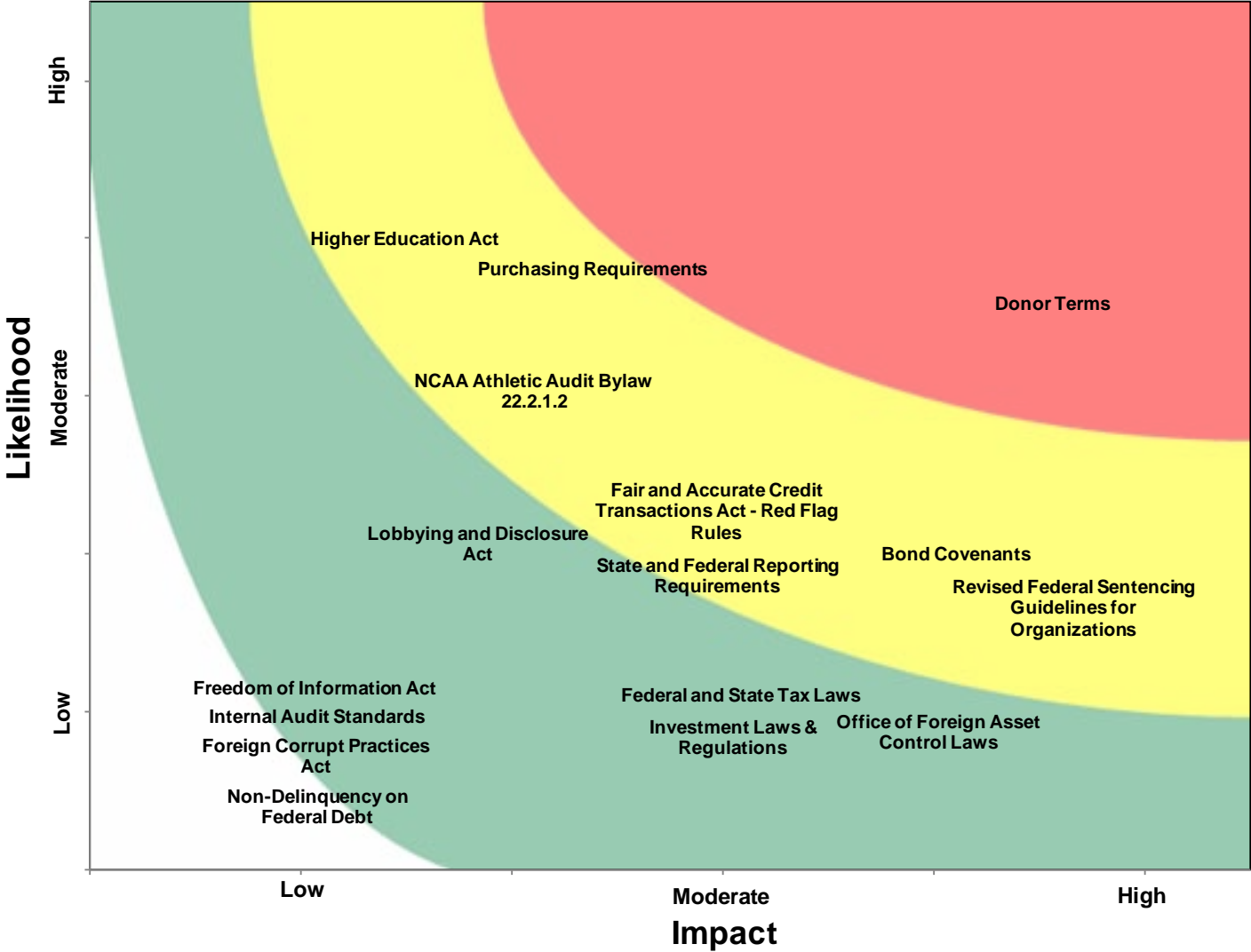
ATHLETICS

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
NCAA/Conference Rules	4	1	Documented policies and procedures
Volumes of rules. Good controls and Mines works for compliance. Violations will have little impact			Training and awareness program
			Compliance program/staff
			Compliance "tone from the top"
			Liaison with the NCAA
			Periodic self-assessment
			Maintain and advertise a compliance hotline
Title IX	1.5	2	Documented policies and procedures
Mines is well above requirements in terms of spending.			Training and awareness program
Non-compliance would require Mines to fix issue.			Compliance program/staff
			Compliance "tone from the top"
			Strategic plan
Tax Laws for Exempt Entities	1	3.5	Documented policies and procedures
Restrictions on types of expenditures			Periodic audits
Restriction on advertising			Tax committee
			Knowledgeable personnel and adequate training
PCI Standards	1	2	Documented policies and procedures
Credit card systems outsourced			Management oversight

ATHLETICS

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
			Periodic audits
			Knowledgeable personnel and adequate training
			E-commerce policies and procedures that are PCI compliant
NCAA Athletics Certification	1	5	Training and awareness program
			Ad hoc athletics certification committee
			Periodic compliance audits
			Compliance program/staff
			Auxiliary oversight committee
Americans with Disabilities Act	1	2	Documented policies and procedures
			Supervisory review and approval
NCAA Fundraising Regulations	2.5	2	Documented policies and procedures
			Management oversight
			Knowledgeable personnel and adequate training

FINANCE AND ADMINISTRATION



FINANCE AND ADMINISTRATION

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
Bond Covenants	2	4	Supervisory review and approval
			Training and awareness program
			Quarterly analysis of bond covenants
State and Federal Reporting Requirements	2	3	Documented policies and procedures
			Tone at the top
			Institutional compliance program
			Identify reporting requirements
			Periodic review and update of laws, rules, and regulations
			Training and awareness program
Purchasing Requirements	4	2.5	Multiple approvals of purchases
Compliance with restrictions caused by federal grants			Procurement card audits
State purchasing laws			Purchasing policies/manual
RFP for purchases greater than \$25k			Robust audit function using CAAT
Payment to employee's business			Separation of duties
Federal Acquisition Regulation			System edits
Utilization of Minority & Women Owned Businesses			Tone at the top
			Independent audit
			Training and awareness program
Investment Laws & Regulations	1	3	Documented policies and procedures

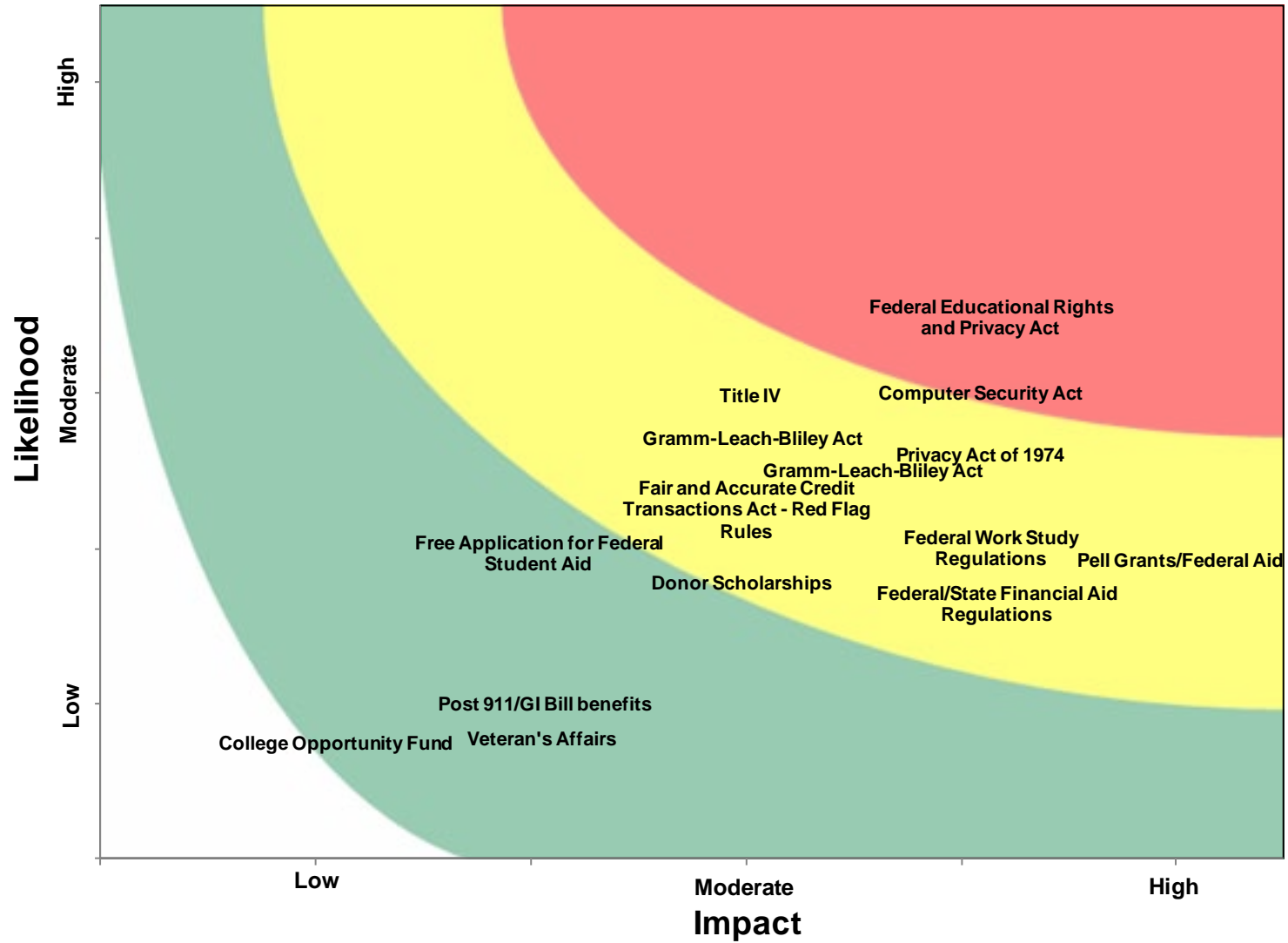
FINANCE AND ADMINISTRATION

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
			Management oversight/ review
			Quality assurance review
Internal Audit Standards	1	1	Develop audit manual in alignment with internal auditing standards
			Conduct internal self-assessments of compliance
			Peer review
Office of Foreign Asset Control Laws	1	4	Training and awareness program
Violating OFAC or other sanctions or embargoes by providing goods or services to countries on the OFAC list			
NCAA Athletic Audit Bylaw 22.2.1.2	3	2	Documented policies and procedures
Rules compliance program must be evaluated by an authority outside the athletics department			Independent audit
Foreign Corrupt Practices Act	1	1	Management review of funds to foreign countries
			Independent audit
Freedom of Information Act	1	1	Training and awareness program
			Management oversight
Higher Education Act	4	1.5	Training and awareness program

FINANCE AND ADMINISTRATION

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
			Conduct internal self-assessments of compliance
Federal and State Tax Laws	1	3	Documented policies and procedures
			Training and awareness program
			Payroll system programming review
			Monitoring of payroll
			Involve expertise of tax professional
Fair and Accurate Credit Transactions Act - Red Flag Rules	2	3	Monitoring
			Training and Awareness Program
			Documented policies & procedures
Donor Terms	3.5	4.5	Internal Audit Function
			Training and Awareness Program
Revised Federal Sentencing Guidelines for Organizations	2	4	Tone at the top
			Documented policies & procedures
Lobbying and Disclosure Act	2	2	Documented policies & procedures
			Management review of reports
Non-Delinquency on Federal Debt	1	1	Documented policies & procedures
			Management Review

FINANCIAL AID



FINANCIAL AID

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
Pell Grants/Federal Aid	2	5	Awards made after FAFSA is verified– Students are awarded but aid is not disbursed until verification is complete.
			Supervisory review of awards and award reports. Audit reports are run at the end census of each semester to verify all aid has been awarded to eligible students. Banner also has awarding rules that do not allow improper awarding, such as a non-resident receiving CO state aid.
			Periodically, test financial aid system
			Build system rules to ensure SARs (Student Aid Reports) are loaded correctly and that all flags from the Dept. of Education are identified appropriately
			System parameters awards only to students that are eligible based on admittance, enrollment, grade level, and need
			Training and Awareness Program Policy and Procedures to eliminate staff errors.
Free Application for Federal Student Aid	2	2	Awards made after FAFSA is verified– Students are awarded but aid is not disbursed until verification is complete.

FINANCIAL AID

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
Institutional Aid Requirements			Supervisory review of awards and award reports. Audit reports are run at the end census of each semester to verify all aid has been awarded to eligible students. Banner also has awarding rules that do not allow improper awarding, such as a non-resident receiving CO state aid.
			Periodically, test financial aid system
			Build system rules to ensure SARs (Student Aid Reports) are loaded correctly and that all flags from the Dept. of Education are identified appropriately
			System parameters awards only to students that are eligible based on admittance, enrollment, grade level, and need
			Training and Awareness Program Policy and Procedures to eliminate staff errors.
Donor Scholarships	2	3	Awards made after FAFSA is verified– Students are awarded but aid is not disbursed until verification is complete.
			Supervisory review of awards and award reports. Audit reports are run at the end census of each semester to verify all aid has been awarded to eligible students.
			Periodically test financial aid system

FINANCIAL AID

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
			Build system rules to ensure SARs (Student Aid Reports) are loaded correctly and that all flags from the Dept. of Education are identified appropriately
			System parameters awards only to students that are eligible based on admittance, enrollment, grade level, and need
			Training and Awareness Program Policy and Procedures to eliminate staff errors.
Federal Work Study Regulations	2	4	Continuous monitoring of off-campus Federal Work Study
			Training and Awareness Program
			Documented policies & procedures -- FWS Coordinator is the individual that is directing the program so fewer mistakes made.
Federal/State Financial Aid Regulations	2	4	Awards made after FAFSA is verified– Students are awarded but aid is not disbursed until verification is complete.
Complete the Fiscal Operations Report and Application to Participate (FISAP)			Supervisory review of awards and award reports. Audit reports are run at the end census of each semester to verify all aid has been awarded to eligible students. Banner also has awarding rules that do not allow improper awarding, such as a non-resident receiving CO state aid.

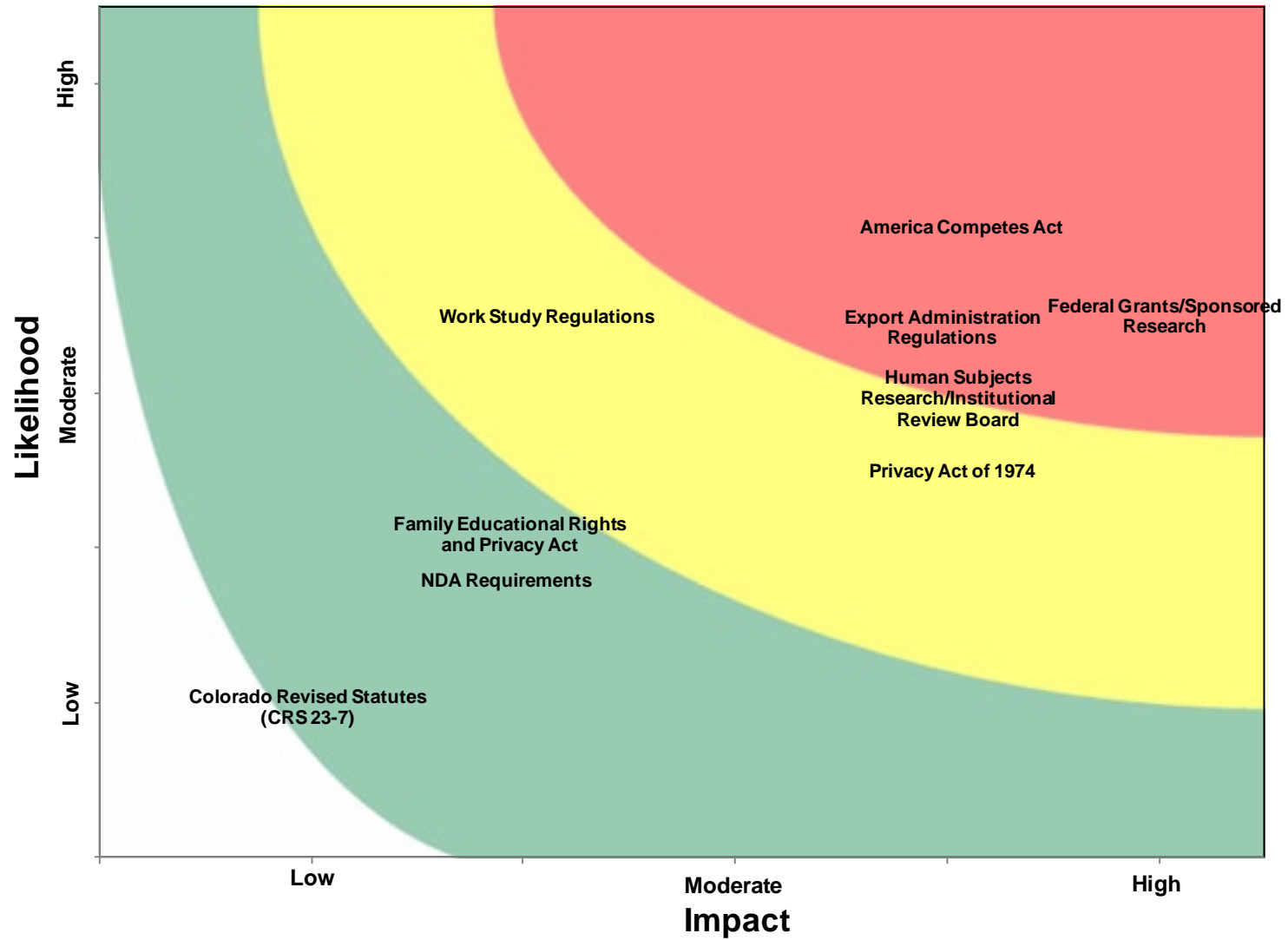
FINANCIAL AID

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
Complete the state Student Unit Record Data System (SURDS)			Periodically test financial aid system
Policies for Drug Law Violations			Build system rules to ensure SARs (Student Aid Reports) are loaded correctly and that all flags from the Dept. of Education are identified appropriately
			System parameters awards only to students that are eligible based on admittance, enrollment, grade level, and need
			Training and Awareness Program Policy and Procedures to eliminate staff errors.
Family Educational Rights and Privacy Act	3.5	4	Documented policies and procedures
			Periodic automatic vulnerability scans of systems, networks, and devices
			Safeguarded storage for electronic data
			Provide FERPA training
			Store hard copy data in secured locations and shred data when no longer needed
			Training and awareness program
Privacy Act of 1974	2.5	4	Documented policies and procedures
			Tone at the top
			Training and awareness program
Computer Security Act	3	4	Documented policies and procedures
			Tone at the top

FINANCIAL AID

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
			Training and awareness program
Post 911/GI Bill benefits	1	2	Monitoring
			Training and awareness program
			Documented policies and procedures
Veteran's Affairs	1	2	Monitoring
			Training and awareness program
			Documented policies and procedures
Fair and Accurate Credit Transactions Act - Red Flag Rules	2	3	Monitoring
			Training and awareness program
			Documented policies and procedures
College Opportunity Fund	1	1	Monitoring
			Training and awareness program
			Documented policies and procedures
Gramm-Leach-Bliley Act	2.5	3	Monitoring
			Training and awareness program
			Documented policies and procedures
Title IV	3	3	Training and awareness program
			Documented policies and procedures
			Documented policies & procedures

GRADUATE STUDIES



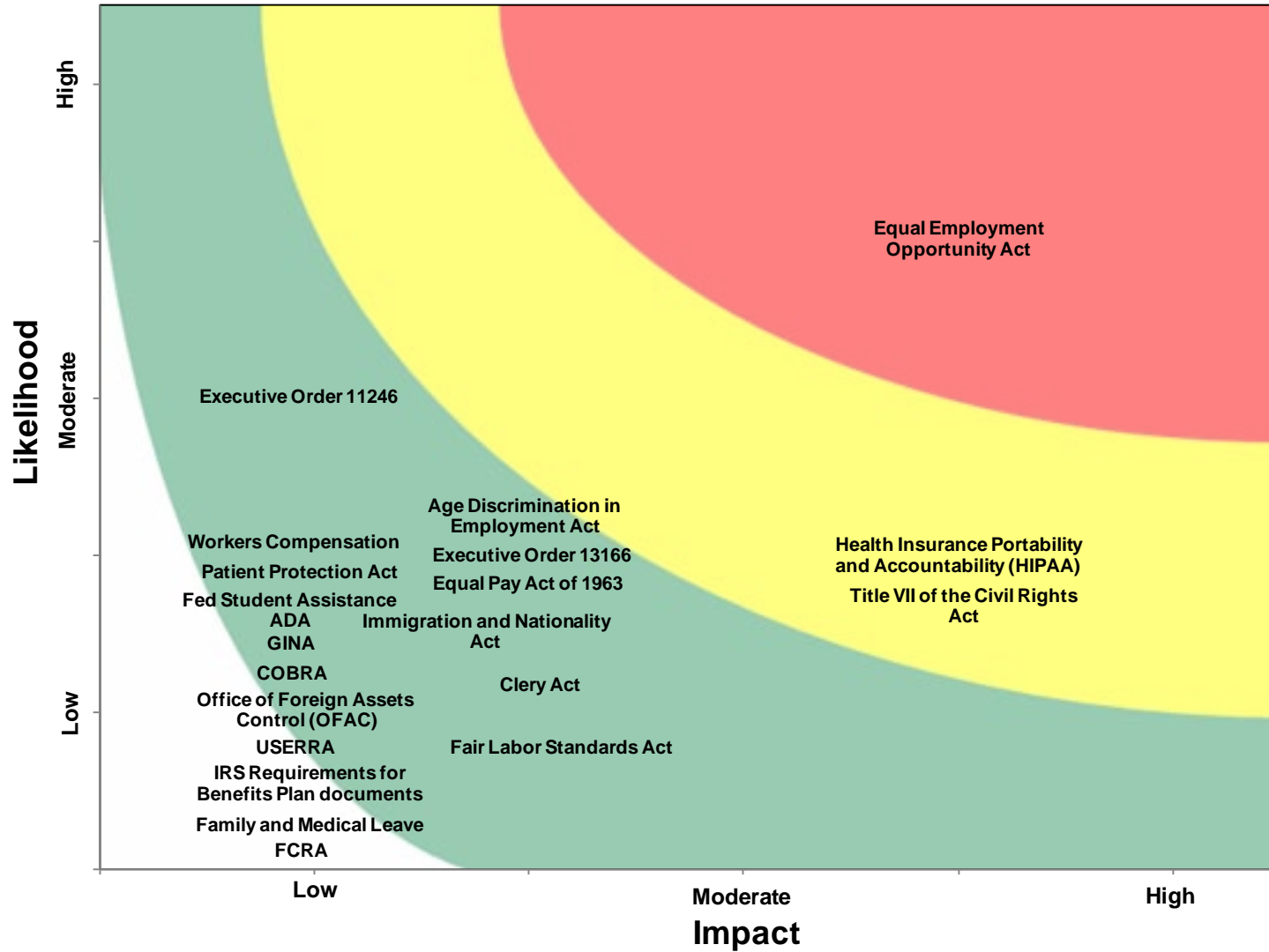
GRADUATE STUDIES

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
Export Administration Regulations	3.5	4.5	Have a research compliance officer perform reviews of activity, protocols, etc.
Export Control Laws			Establish export control compliance person
International Traffic in Arms Regulations			Implement an approval process for exporting items
NDA Requirements	2	2	Legal counsel review
Non-disclosure Agreements			Training and awareness program
Colorado Revised Statutes (CRS 23-7)	1	1	Training and awareness
Classification of students - residency			Management oversight
America Competes Act	4	4	Policies and procedures
			Documentation of practices
			Regular Review
Privacy Act of 1974	2.5	4	Documented policies and procedures
			Tone at the top
			Training and awareness program
Family Educational Rights and Privacy Act	2	2	Documented policies and procedures
			Periodic automatic vulnerability scans of systems, networks, and devices
			Safeguarded storage for electronic data
			Provide FERPA training
			Store hard copy data in secured locations and shred data when no longer needed
			Training and awareness program

GRADUATE STUDIES

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
Human Subjects Research/Institutional Review Board	3	4	Training and awareness
			Establish Institutional Review Board
Federal Grants/Sponsored Research	3.5	5	Regular transaction review
			Independent review of expenditures
			Training and awareness
			Provide accurate and timely accounting
Work Study Regulations	3.5	2	Legal counsel review
			Training and awareness program
			Management oversight

HUMAN RESOURCES



HUMAN RESOURCES

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
Immigration and Nationality Act	1.5	1.5	Documented policies and procedures
Maintain appropriate immigration status for faculty, scholars, and staff			Training and awareness program
			Monitor immigration status
			Develop communication mechanism with affected faculty and staff
			Monitor compliance with foreign national requirements
Health Insurance Portability and Accountability (HIPAA)	2	4	Collaboration between privacy officer and research administrators
			HIPAA training - HR Privacy Officer is our Benefits Manager who arranges training and provides periodic in-service to HR/Payroll staff
			Mines employee health insurance plans are not a covered entity; business associate only for insured benefits.
			Internal protocols, locked cabinets for benefits files
			Proper security of e-files containing covered data
			Use of vendor secure e-mail site for rare occurrences of exchanging PHI
Office of Foreign Assets Control (OFAC)	1	1	All new hires will be screened against federal exclusion and debarment lists

HUMAN RESOURCES

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
Violating OFAC by hiring an employee who appears on the governmental list of restricted parties			For all foreign vendors, verify that a country is not excluded
USERRA	1	1	Training and awareness program
Uniformed Services Employment and Reemployment Rights Act (USERRA) - laws regarding military leave			Monitor veteran hiring and employment status
Clery Act	1	2	Annual review of plans
Emergency preparedness and disaster recovery			Training and awareness program
			Annual review of plans
			All systems are backed up (monthly full, weekly and daily incrementals) and tapes are stored off site in case of a disaster
			High availability systems are redundant in that they are split between computer rooms on campus
			Use standard off the shelf hardware so it can be replaced fairly quickly
Executive Order 11246	3	1	
Office of Federal Contract Compliance Programs			Contracts with Mountain States Employers Council for AA Plan updates
Affirmative Action and associated requirements			Obtains compensation analyses from MSEC

HUMAN RESOURCES

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
Affirmative Action plan – annual update			Perform internal testing – some statistical explanation, some situational reviews
			Obtains hire, promotion, and termination analyses from MSEC
IRS Requirements for Benefits Plan documents	1	1	
			Establishment and periodic review of benefits plan documents
			Non-discrimination testing where required
			Plans affected include Section 403(b) – voluntary tax deferred annuities – and Section 125 – cafeteria plan for tax exempted benefits (medical flexible spending account)
			Monitor regulatory changes, update plans – 403(b) has periodic legal review; 125 is contracted through plan vendor
Executive Order 13166	2	2	Access to services
Limited English Proficiency			Conduct 4 factor analysis
Aimed at primary services - academic & student			Establish policy for access to services and assign resources to support
Fair Labor Standards Act	1	2	
Exemption status of jobs	1	2	HR review of job descriptions during state exemption process
Timekeeping records that support pay			Departments to certify job descriptions

HUMAN RESOURCES

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
			Split responsibility HR and Payroll
COBRA	1	1	
			Protocols and policies in place
			Integrated updates to rules with state DPA and benefits consultants
Family and Medical Leave	1	1	
Regulations and state personnel rules			Periodic review of policies and protocols
			Leave system tracks
			Coordination with supervisors
ADA	1	1	Protocol in place
Americans with Disabilities Act			Procedures under review at Legal Services
			Once final, promulgate and distribute
			Essential function analyses completed on most jobs with physical demands
			Post offer, pre-employment functional capacity evaluations obtained for those in jobs with physical demands
GINA	1	1	Genetic information never a part of any employment decision – not an issue unless federal regulations change – monitor status only
Genetic Information Nondiscrimination Act			

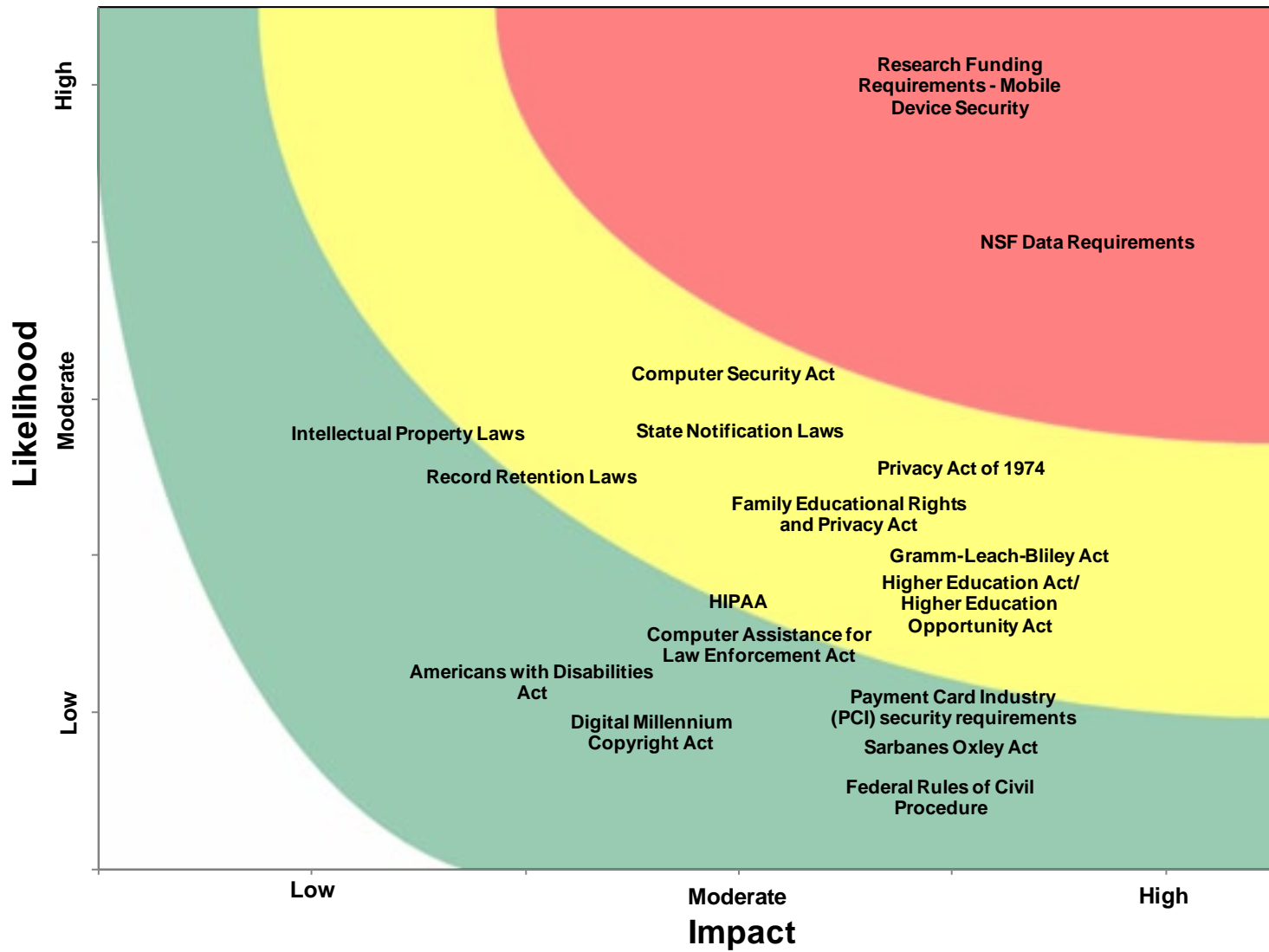
HUMAN RESOURCES

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
Fed Student Assistance	1	1	Compensation decisions do not include commissions, bonuses, or other incentives based upon numbers of students admitted or on amounts of financial aid awarded
US Department of Education Incentive Compensation Regulations – 34 CFR Part 668.14(b)			
Patient Protection Act	1	1	Working with benefits consultants, insurers and DPA, monitor implementing regulations – currently in full compliance
PPACA - Patient Protection and Affordable Care Act			
FCRA	1	1	Background Checks
Fair Credit Reporting Act			Policy in place
			Agreement with vendor
			Conformity with obtaining authorizations
			Secure reports – locked cabinet
Workers Compensation	1	1	Meet state statutory standards for having at least two designated providers
			Issue Rule 8 letters timely
			Supervisor training – periodic information sent via email; developing materials to be available by year end 2011
Equal Employment Opportunity Act	4	4	Documented policies and procedures

HUMAN RESOURCES

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
			Monitoring
			Training
Title VII of the Civil Rights Act	2	4	Documented policies and procedures
			Monitoring
			Training
Equal Pay Act of 1963	2	2	Documented policies and procedures
			Monitoring
			Independent Audit
Age Discrimination in Employment Act	2	2	Documented policies and procedures
			Monitoring
			Independent Audit

INFORMATION TECHNOLOGY



INFORMATION TECHNOLOGY

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
Digital Millennium Copyright Act	1	2.5	Assign the responsibility to monitor compliance of licenses to a specific function
			Establish policies and procedures for licensing and using technology/software
Intellectual Property Laws	3	1.5	Assign the responsibility to monitor compliance of licenses to a specific function
Properly license technologies/software			Establish policies and procedures for licensing and using technology/software
Payment Card Industry (PCI) security requirements	1	4	Management review/oversight
			Vendor contract review and enforcement
Research Funding Requirements - Mobile Device Security	5	4	Centralized accounting of access
			Annual review of remote access
Record Retention Laws	2.5	2	Annual review of requirements
			Backups and archives
			Maintain IT staff skills
			Vendor contract review and enforcement
HIPAA	1.5	3	Training and awareness program
			Documented Policies and procedures
Family Educational Rights and Privacy Act	2.5	3.5	Documented policies and procedures
			Periodic automatic vulnerability scans of systems, networks, and devices

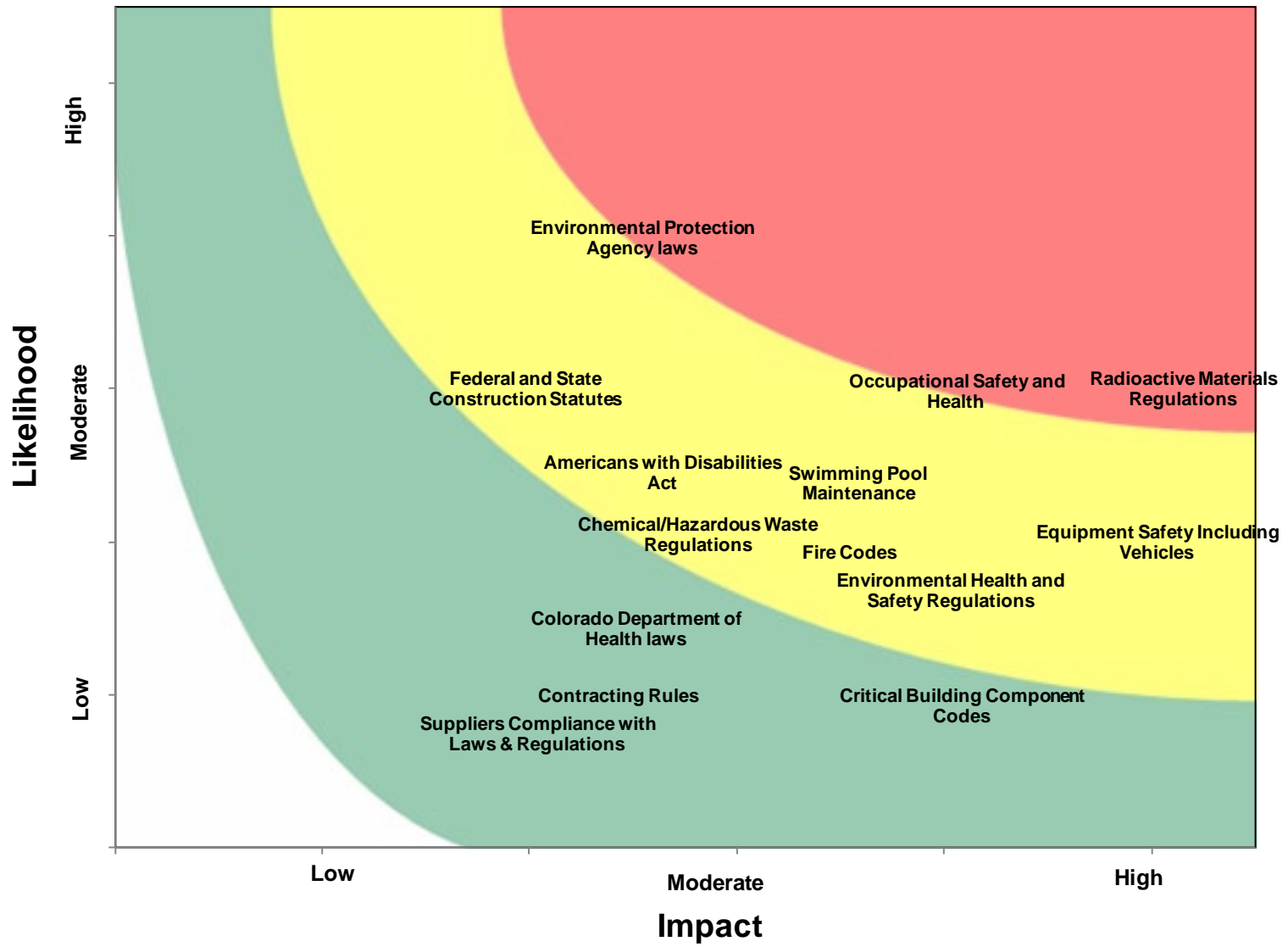
INFORMATION TECHNOLOGY

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
			Safeguarded storage for electronic data
			Provide FERPA training
			Store hard copy data in secured locations and shred data when no longer needed
			Training and awareness program
Privacy Act of 1974	2.5	4	Documented policies and procedures
			Tone at the top
			Training and awareness program
NSF Data Requirements	4	5	Documented policies and procedures
Compromise of regulated, sensitive, or confidential data			Training and awareness program
			Encryption of devices and data
			Centralized, server-based storage
			Password management
			Firewalls, VLANs, VPN
			Vendor contract review and enforcement
			Physically secure server and network rooms
Computer Security Act	3	3	Documented policies and procedures
			Tone at the top
			Training and awareness program
State Notification Laws	3	3	Documented policies and procedures
			Training and awareness program
Americans with Disabilities Act	1	2	Augmented listening hardware

INFORMATION TECHNOLOGY

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
			Specialized monitors and software for visually impaired users
			Special tables for wheelchairs
			Accommodation policies and practices
Federal Rules of Civil Procedure	1	4	Documented Policies and procedures
			Legal review
			IT staff training
Higher Education Act/ Higher Education Opportunity Act	2	4	Functional area management
			Properly maintained supporting IT resources
Gramm-Leach-Bliley Act	2	4	Designated information security officer
			Infosec program
			Documented Policies and procedures
			Training and awareness program
Sarbanes Oxley Act	1	4	Documented Policies and procedures
			Legal review
			IT staff training
Computer Assistance for Law Enforcement Act	1	3	Properly maintained supporting IT resources

PLANT OPERATIONS



PLANT OPERATIONS

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
Contracting Rules	1	2.5	Documented policies and procedures
			Supervisory review and approval
			Training and awareness program
			Award committee review and approval for large contracts
Fire Codes	2	3.5	Resource analysis
			Evaluation of assignments
Occupational Safety and Health Generator maintenance required	3	4	Training and awareness program
			Supervision
Asbestos - potential in Green Center			Asbestos Awareness Training - Personnel require 2-hour awareness training for employees working in a building with asbestos containing building materials. Training provided by EHS.
			Asbestos Building Inspector - Maintain an employee who is trained in the identification and sampling of asbestos containing building materials. Sampling services provided by EHS or licensed state certified building inspector. Required before renovation/repair work.
			Signage
			Insurance
			Protective gear
			Periodic maintenance
Critical Building Component Codes	1	4	Scheduled maintenance

PLANT OPERATIONS

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
HVAC, elevator, lifts boilers			Proper routine inspections
			Review of maintenance contracts
Swimming Pool Maintenance	2.5	3.5	Training and certification
			Periodic maintenance
Federal and State Construction Statutes	3	2	Inspections
Building and construction codes in academic facilities			Bids identifying statutes
			Contracts identifying statutes
Environmental Protection Agency laws	4	2.5	Training and awareness program
CSMRI, Mines outside of school			Periodic random inspections
Resource Conservation and Recovery Act (RCRA)			
Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA)			
Storm Water Reports			Conduct visual inspection of storm water run-off controls at the Edgar Mine and Joe Reynolds claim. Submit report to CDPHE.
Community Right-to-Know			By March 31 of each year provide emergency planning committees with information about chemicals on main campus and at the Edgar Mine.
CFC Equipment Registration and Technician Certification			Register CFC containing equipment annually. Renew certifications for state registered CFC technicians.

PLANT OPERATIONS

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
Spill Prevention, Control and Countermeasure Plan			Maintain spill prevention and emergency response plan for petroleum spills from emergency generators, fuel tank, gasoline storage tank, and used oil tank.
City of Golden Water Permits	3	2	Training and awareness program
Wastewater Discharge Permit			Perform quarterly monitoring of wastewater from campus buildings. Submit sampling report to City of Golden. Submit annual spill reports to the City of Golden.
Colorado Department of Health laws	1.5	2.5	Training and awareness program
Swimming pool, eateries			Periodic random inspections
Americans with Disabilities Act	2.5	2.5	Documented policies and procedures
			Supervisory review and approval
Equipment Safety Including Vehicles	2	5	Safety training
Licenses required			License verification
Monitoring of eligibility			Training
			Policies
Chemical/Hazardous Waste Regulations	2	3	Training and awareness program
Chemical Facility Anti-Terrorism Standards (CFATS)			Supervision
			Signage
			Protective gear
			Certifications as applicable and training

PLANT OPERATIONS

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
Hazardous Waste Biennial Report			Submit report to CDPHE on total volume of hazardous waste generated on campus during odd numbered years.
Ship Hazardous Waste Every 90 Days			EHS arranges transportation and disposal with licensed waste disposal contractors.
Hazardous Materials Shipments			Manage dangerous goods shipments for campus personnel. Maintain current training for surface or air shipments of hazardous materials for all campus personnel.
Remove Hazardous Waste From Laboratory Satellite Accumulation Areas			EHS employees remove waste from labs and transports to 90 day storage areas.
Maintain Hazardous Waste Contingency Plan			Maintain emergency response contracts, written response procedures and distribute plans to City of Golden emergency services, Jefferson County emergency planning and local emergency care facility
Provide cradle to grave tracking of hazardous waste			Maintained by EHS using Waste Tracking database.
Maintain a waste minimization plan			Maintained by EHS. Last Revision 2008.
Provide annual training for Generators of hazardous waste			Training provided by EHS. Training tracked using EHS Training database.
Conduct weekly Inspections of 90 day waste storage facilities			Inspections conducted by EHS.
Identify/hazard classify chemical wastes			Completed by EHS for wastes submitted by teaching, research, and maintenance activities.

PLANT OPERATIONS

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
Container Management			Maintain waste storage containers in good condition. Ensure waste is compatible with containers, track storage start dates.
Record Keeping			Maintain waste manifests, Land disposal restriction notices, biennial reports, waste analysis, and waste characterization data.
Radioactive Materials Regulations	3	5	Training and awareness program
Maintain Materials License			Radiation Safety Officer Maintains license for radioactive materials (RAM) and radiation producing equipment (RPE) on CSM campus. Permit renewal – Every 5 years. Maintain RAM and RPE inventory.
Material License Amendments			License amendments are required any time a change to the type or quantity of radioactive materials used or stored on campus changes. All license amendments require CDPHE approval prior to implementing change.
Radiation Producing Equipment – Equipment and Facility Registration Responsibilities			Radiation safety and machine operation training of individuals. Maintain training records for three years. Maintain records of personnel qualifications to use RAM and RPE.
Occupational Dose Limits			Licensee is required to monitor external and internal occupational doses of adults, minors, and pregnant women in accordance with 4.18.

PLANT OPERATIONS

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
Testing for Leakage of Contamination of Sealed Sources			Perform sealed source leak tests in accordance with CDPHE testing intervals. Typically 3 or 6 month intervals depending upon type and activity of the source material.
Surveys and Monitoring			Instruments and equipment used for quantitative radiation measurements are calibrated at intervals not to exceed 12 months.
Record Keeping Requirements			Comply with CDPHE radiation safety program recordkeeping requirements. (1) Records of radiation protection program, (2) Records of surveys, (3) Records of tests for leakage or contamination of sealed sources, (4) Records of prior occupational dose, (5) Records of planned special exposures, (6) Records of individual monitoring results, (7) Records of dose to individual members of the public, (8) Records of waste disposal, (9) Records of testing entry control devices for very high radiation areas., (10) Maintain Training records, (11) Maintain RPE inspection records, (12) Maintain RAM transportation records.
Maintain a Radiation Protection Program			Develop and implement radiation protection program that uses engineering controls, procedural controls and sound radiation protection principals that achieve occupational doses and doses to the general public that are as low as reasonably achievable. Program review is required at 12 month intervals.

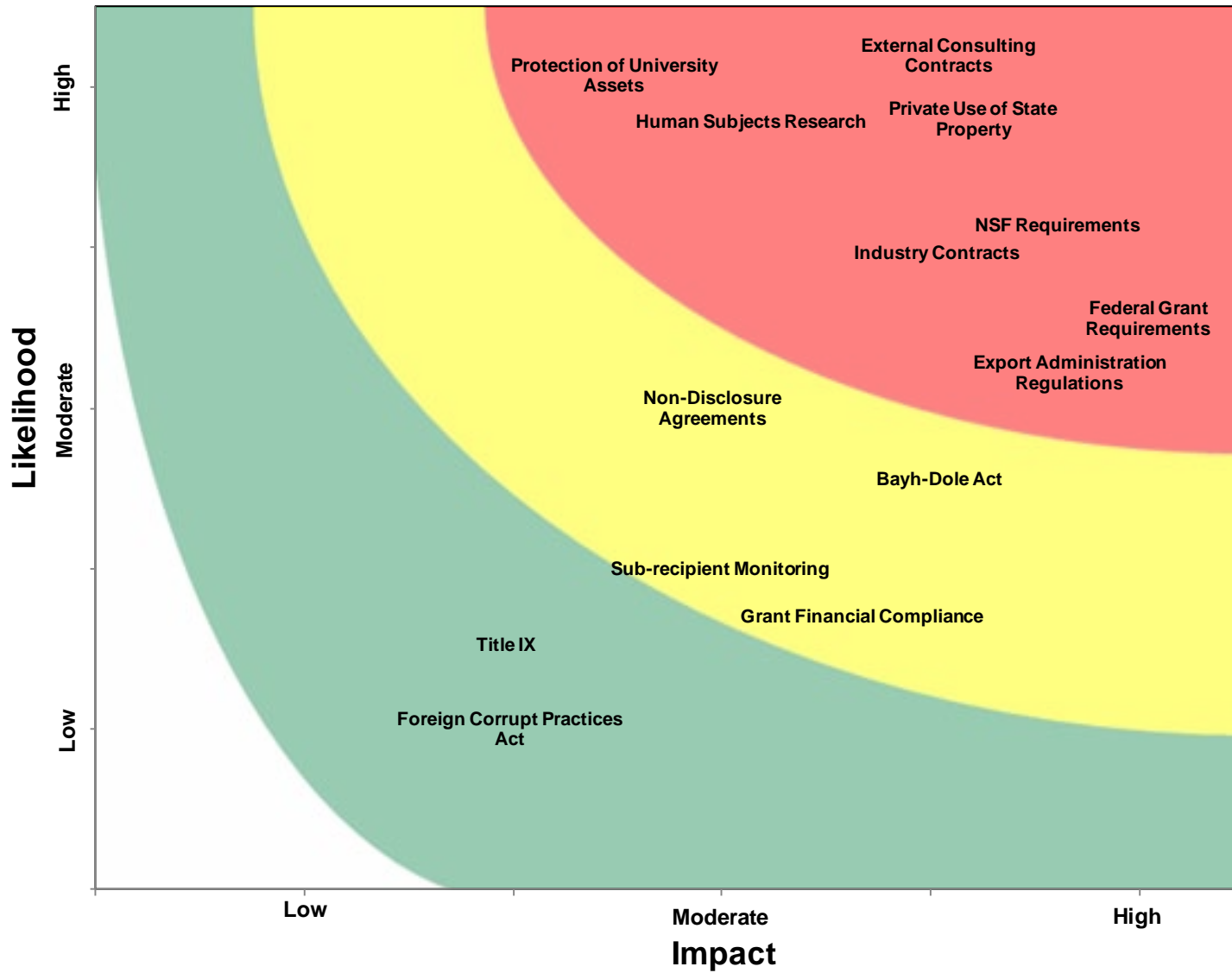
PLANT OPERATIONS

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
Storage and control of licensed or registered sources of radiation			Prevent unauthorized removal or access to licensed or registered sources of radiation and radiation producing equipment.
Radioactive waste disposal			Maintain waste profiles, site use permits, low level waste export permits, for the transportation and disposal of radioactive materials. Notify the CDPHE of final receipt and disposal of radioactive waste materials at licensed disposal facility.
Incident notification			Notify the CDPHE of the following: <ol style="list-style-type: none"> 1. Incident of exposure that exceeds regulatory limits 2. An event involving the loss of control of a licensed or registered source of radiation 3. Release of radioactive material inside or outside a restricted area 4. An unplanned contamination event 5. An event where equipment is disabled or fails to function as designed 6. Incident that requires medical treatment.
Radiation producing materials - Transportation			Survey incoming packages that contain radiation producing equipment. Package and ship radiation producing materials following Department of Transportation packaging and hazardous materials shipping regulations.
			Signage
			Protective gear

PLANT OPERATIONS

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
Suppliers Compliance with Laws & Regulations	1	2	Supervision
			Certifications as applicable and training

RESEARCH AND ADMINISTRATION



RESEARCH AND ADMINISTRATION

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
Federal Grant Requirements	3.5	5	Supervisory review and approval
OMB Circular A-110: Administrative Requirements including reporting, procurement, and codes of conduct			Hire knowledgeable personnel and provide adequate training
OMB Circular A-21: Cost principles for educational institutions			Establish and document procedures to ensure that funds are acquired, expended, and monitored in accordance with the grant agreement
Other OMB Guidance			Monitor vendors against the Federal Government's Debarment and Suspension list
Lack of formal grants proposal process/inability to enforce grants policies and procedures			Assign a responsible party for all federal grants
Appropriate grant closeout procedures are not followed			Implement regular audit procedures
Sub-recipient Monitoring	2	3	Documented policies and procedures
OMB Circular A-133			Appoint personnel to monitor sub-grantee compliance with terms of the agreements
			Maintain updated records from all sub-grantees
			Train sub-grantees on all requirements
			Exhibit proper tone at the top
			Establish consequences for non-compliance
			Institute PI review and approval
			Hire knowledgeable personnel and provide adequate training

RESEARCH AND ADMINISTRATION

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
			Centralized grant reporting function
Bayh-Dole Act	2.5	4	Independent audit
Technology transfer requirements			Training and awareness program
Foreign Corrupt Practices Act	1	2	Management review of funds to foreign countries
			Independent audit
Export Administration Regulations	3.5	4.5	Have a research compliance officer perform reviews of activity, protocols, etc.
Export Control Laws			Establish export control compliance person
Data traveling out of the country			Implement an approval process for exporting items
International students viewing unauthorized data			
Private Use of State Property	5	4	Segregation of contracting/procurement duties
Conflict of Interest; using school property for private use, particularly in consulting arrangements			Signed conflict of interest statements for all Principal Investigators
			Related-party disclosure statement
			Proper monitoring by department leads
Protection of University Assets	5	2.5	Documented policies and procedures
The university should be charging for proper use			Training and awareness program
			Compliance "tone from the top"
Grant Financial Compliance	2	3.5	Management oversight
Unallowable costs charged to grant	2	2	Documented policies and procedures

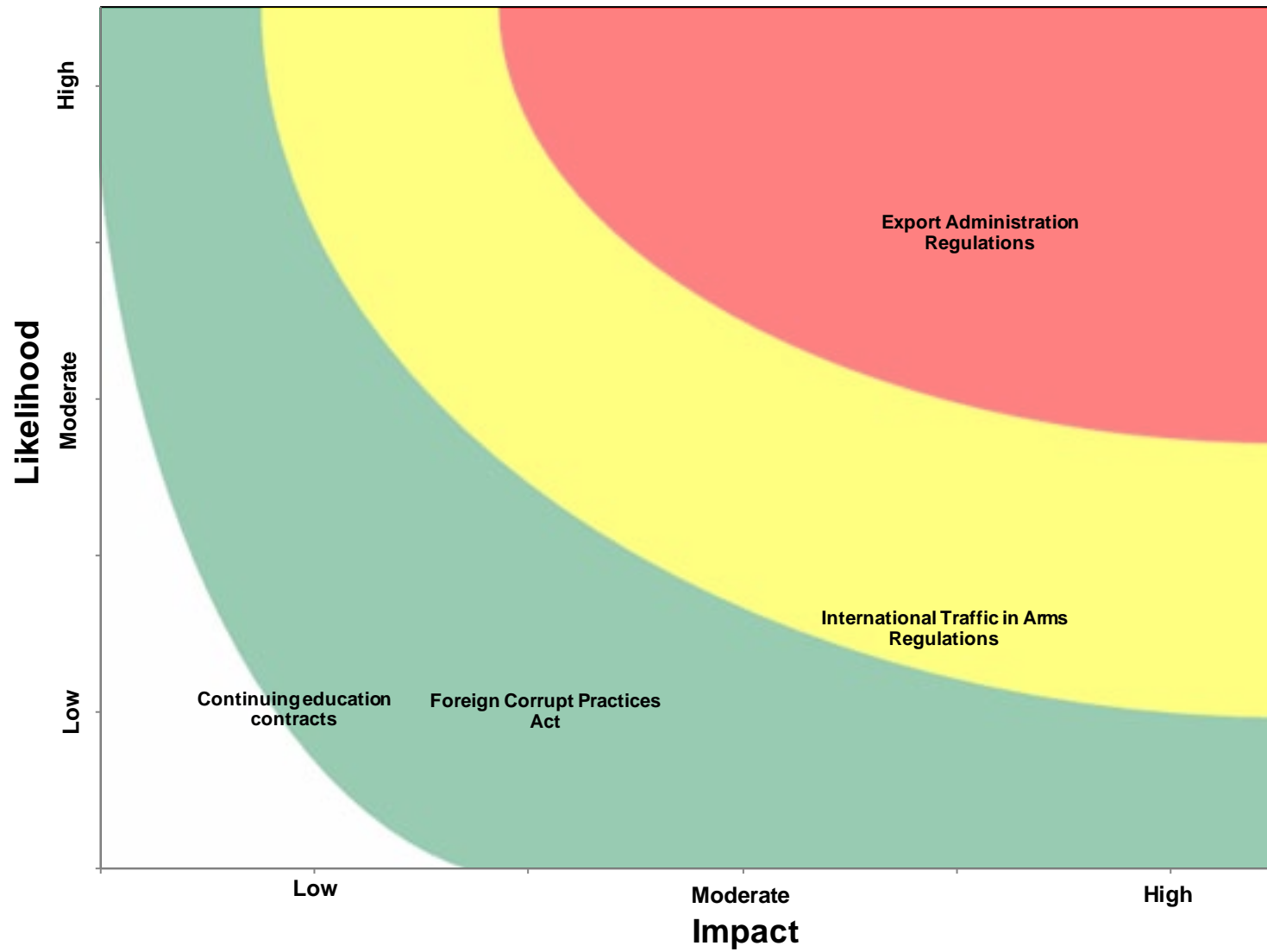
RESEARCH AND ADMINISTRATION

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
Non-compliance with OMB Circular A-21 (Cost principles for grants) and other regulations and laws	2	2	Careful independent monitoring of costs
Violation of research salary cap limitations	1	1	Training for PIs to understand their vital role in accounting for charges
Program measures not met, but funds used	1	3	Periodic reviews/audits
Appropriate approvals are not documented for grant/contract purchases	1	2	Third party review prior to payment
			Training and awareness program
			Review of budget by pre-awards office
			Conduct annual review of total salaries
			Monitoring by grant accounting office
			Review to ensure expenses are appropriate and allowable
Title IX	1.5	2	Documented policies and procedures
Mines is well above requirements in terms of spending.			Training and awareness program
Non-compliance would require Mines to fix issue.			Compliance program/staff
			Compliance "tone from the top"
			Strategic plan
External Consulting Contracts	5	4	Documented policies and procedures
			Training and awareness program
			Compliance program/staff
			Compliance "tone from the top"

RESEARCH AND ADMINISTRATION

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
Industry Contracts	4	4	Documented policies and procedures
			Training and awareness program
			Compliance program/staff
			Compliance "tone from the top"
Human Subjects Research	5	3	Documented policies and procedures
Need Institutional Review Board			Compliance program/staff
Non-Disclosure Agreements	3	3	Documented policies and procedures
			Training and awareness program
			Legal review
NSF Requirements	4	4.5	Documented policies and procedures
Mentoring of Post-docs			Training and awareness program
Data management policies			

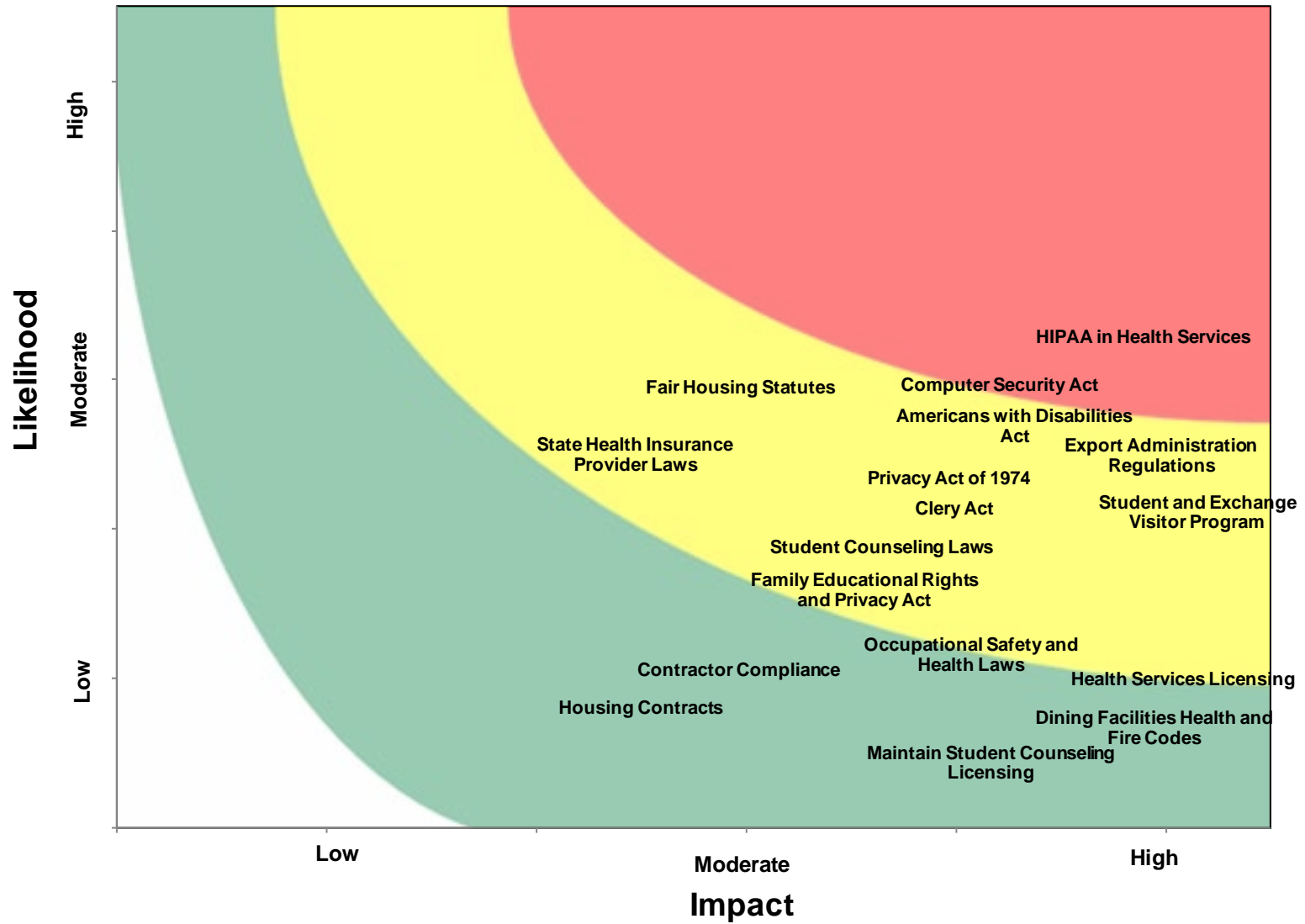
STRATEGIC OPERATIONS



STRATEGIC OPERATIONS

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
Continuing Education Contracts	1	1	Documented policies and procedures
			Training and awareness program
Export Administration Regulations	4	4	Have a research compliance officer perform reviews of activity, protocols, etc.
Export Control Laws			Establish export control compliance person
International Traffic in Arms Regulations			Implement an approval process for exporting items
International Traffic in Arms Regulations	1.5	4	Have a research compliance officer perform reviews of activity, protocols
			Establish export control compliance person
			Implement an approval process for exporting items
Foreign Corrupt Practices Act	1	2	Management review of funds to foreign countries
			Independent audit

STUDENT LIFE



STUDENT LIFE

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
Fair Housing Statutes	3	3	Documented policies and procedures
Maintain housing according to laws and regulations, including the fair housing statute			Routinely evaluate new rules
			Routinely conduct facility evaluations
			Review code checklist during facilities construction
			Review inspection reports to ensure appropriate actions were taken
Americans with Disabilities Act	2.5	4	Documented policies and procedures
			Routinely evaluate new rules
			Assign oversight responsibility to individual or department
			Have an ADA compliance component in construction process
Housing Contracts	1	2.5	Training and awareness program
			Adequate disclosure of contract terms
Student and Exchange Visitor Program	2	5	Documented policies and procedures
Student and Exchange Visitor Information System (SEVIS) reporting requirements			Training and awareness program
			Monitor compliance
Family Educational Rights and Privacy Act	2	3.5	Documented policies and procedures
Procedures should be created for release of information from campus security			Periodic automatic vulnerability scans of systems, networks, and devices
			Safeguarded storage for electronic data

STUDENT LIFE

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
			Provide FERPA training
			Store hard copy data in secured locations and shred data when no longer needed
			Training and awareness program
Privacy Act of 1974	2.5	4	Documented policies and procedures
			Tone at the top
			Training and awareness program
Computer Security Act	3	4	Documented policies and procedures
			Tone at the top
			Training and awareness program
Contractor Compliance	1	3	Contracts and services should be monitored for terms and conditions
			Contracts should include inspection and right to audit clauses
			Contracts should have measurable terms
			Assign responsibility for contract monitoring
Student Counseling Laws	2	3.5	Training and awareness program
Student Counseling Confidentiality			Documented policies and procedures
Colorado Revised Statutes 12-43			Periodic automatic vulnerability scans of systems, networks, and devices
			Safeguarded storage for electronic data
			Store records in secure locations and shred records when disposing
Maintain Student Counseling Licensing	1	4	Documented policies and procedures

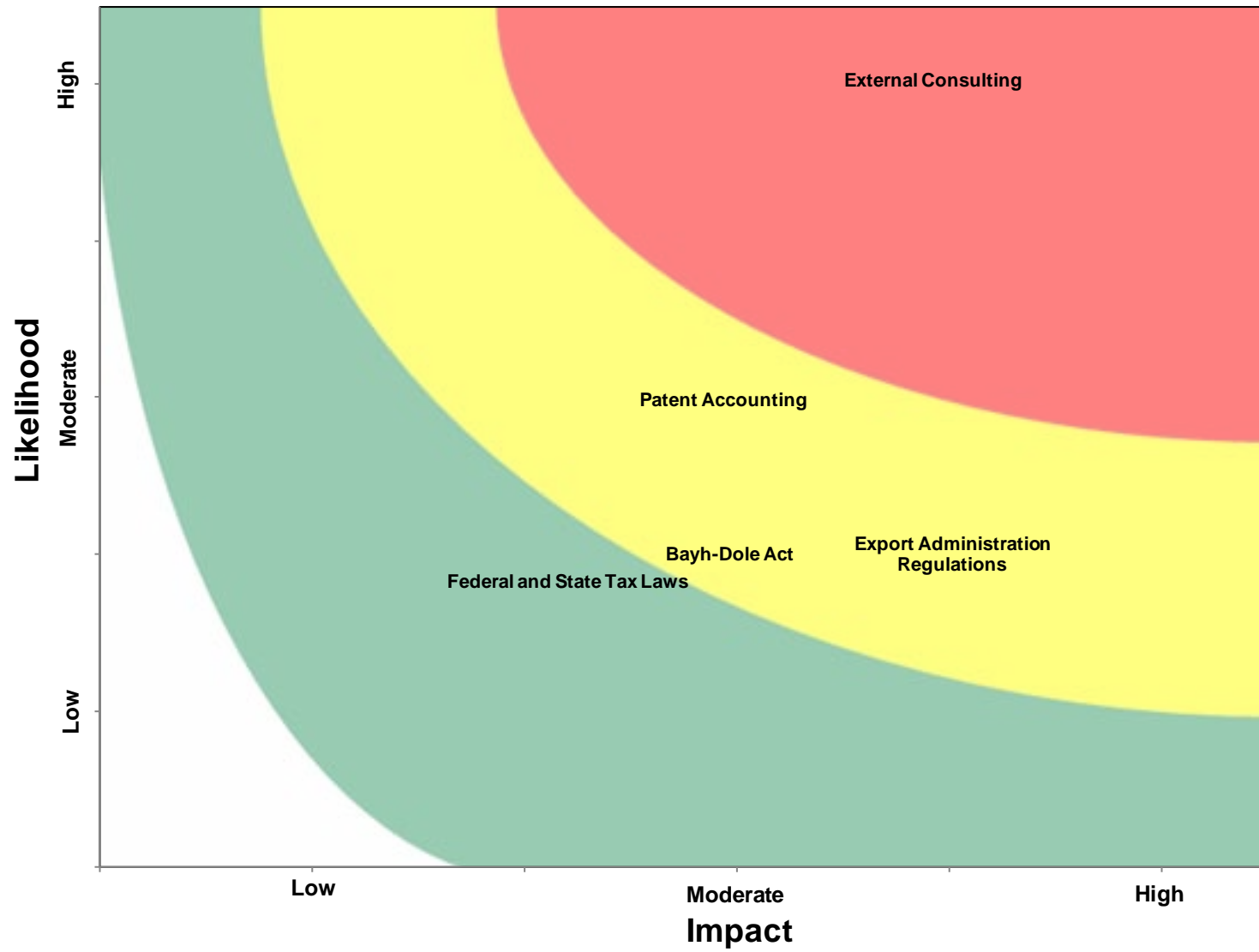
STUDENT LIFE

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
			Perform annual reviews of licensing requirements
			Initial and continued review of licensing requirements
Dining Facilities Health and Fire Codes	1	5	Documented policies and procedures
			Provide safety and hygiene training to employees
			Evaluate for update of facilities and organization of faculty
			Periodic in-house safety inspections
			Posted material safety data sheets and temperature charts
			Training and awareness program
			Provide incentives for compliance with health code
			Post safety information
			Include health code compliance in job descriptions
HIPAA in Health Services	3	5	Access controls
			Record retention and destruction policies
			Compliance program/staff
			Training and Awareness Program
			Documented policies & procedures
Health Services Licensing	1	5	Audit staff files for appropriate licensing and/or continuing education

STUDENT LIFE

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
			Perform annual reviews of licensing requirements
			Perform criminal background and reference checks on new employees
			Documented policies & procedures
Clery Act	2	4	Annual review of plans
Comply with state and federal laws regarding emergency preparedness and disaster recovery			Training and awareness program
Export Administration Regulations	2	5	Training and awareness program
			Documented policies & procedures
Occupational Safety and Health Laws	1	4	Training and awareness program
			Documented policies & procedures
State Health Insurance Provider Laws	2.5	2.5	Training and awareness program
			Documented policies & procedures

TECHNOLOGY TRANSFER



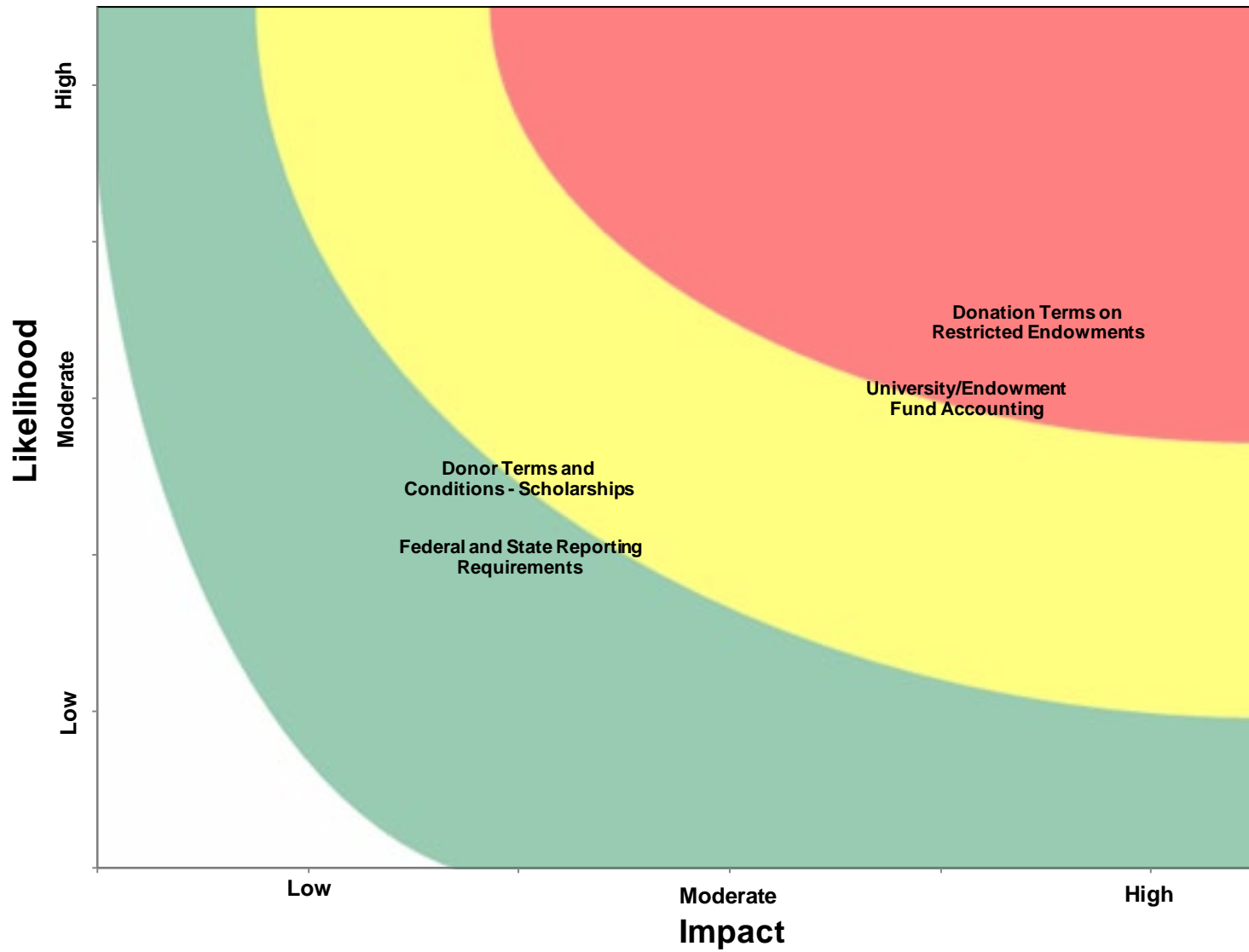
TECHNOLOGY TRANSFER

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
Bayh-Dole Act	2	3	Documented policies and procedures
Universities must file patents on inventions they own			Accounting review
Government retains march-in rights			
Preference in licensing must be given to small business			
Timelines on disclosing invention, election to retain title, and filing of patent			
Export Administration Regulations	2	4	Have a research compliance officer perform reviews of activity, protocols, etc.
Export Control Laws			Establish export control compliance person
Data traveling out of the country			Implement an approval process for exporting items
International students viewing unauthorized data			
Patent Accounting	3	3	Documented policies and procedures
			Audit
External Consulting	5	4	Documented policies and procedures
Disclosure of Outside Financing			Training and awareness program
Conflict of interest			Compliance program/staff
Control over consulting contracts			Compliance "tone from the top"
Federal and State Tax Laws	2	2	Documented policies and procedures

TECHNOLOGY TRANSFER

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
External companies are not allowed to be hosted on campus due to non-exempt tax status			Training and awareness program
			Payroll system programming review
			Monitoring of payroll
			Involve expertise of tax professional

UNIVERSITY ADVANCEMENT



UNIVERSITY ADVANCEMENT

COMPLIANCE REQUIREMENT	LIKELIHOOD	IMPACT	POTENTIAL MITIGATING CONTROLS
Donor Terms and Conditions - Scholarships	2.5	2	Review and approval of expenditures
			Trained staff with regard to donor restrictions
			Standard language for donor agreements and restrictions
			Approval process for restricted gifts
Donation Terms on Restricted Endowments	3.5	4.5	Review and approval of expenditures
			Trained staff with regard to donor restrictions
			Standard language for donor agreements and restrictions
			Approval process for restricted gifts
University/Endowment Fund Accounting	3	4	Documented policies and procedures
			Segregation of duties
			Donor reports
			Management review of expenditures against donor wishes
			Training and awareness program
Federal and State Reporting Requirements	2	2	Documented policies and procedures
			Tone at the top
			Institutional compliance program
			Identify reporting requirements
			Periodic review and update of laws, rules, and regulations
			Training and awareness program

Section 4 – Links to Key Laws and Regulations

Academic Affairs

Intellectual Property and Trademark Laws

- Copyright laws provide federal protection against infringement of certain exclusive rights, such as reproduction and distribution, of “original works of authorship,” including computer software, literary works, musical works, and motion pictures. The use of a commercial brand to identify a product is protected by trademark law, which prohibits the unauthorized use of “any word, name, symbol, or device” used by a person “to identify and distinguish his or her goods, including a unique product, from those manufactured or sold by others and to indicate the source of the goods.” Finally, trade secret law provides legal protection for any formula, device, or compilation of information used in a business from being disclosed without the owner’s permission. However, legal protection is only afforded to those trade secrets that possess independent economic value and which the owner has taken reasonable measures to keep secret.
- <http://www.uspto.gov/ip/global/enforcement/index.jsp>

Export Administration Regulations (EAR)

- EAR govern the lawful export of most commercial items, including when non-U.S. persons or foreign nationals can be granted access to regulated products or technology by a U.S. company or institution of higher education. Under the "deemed export" rule, allowing non-U.S. persons or foreign nationals access to the product or technology may trigger the requirement to apply for a license prior to that access. There is an exemption for fundamental research that is codified at [15 C.F.R. § 734.8](#).
- Export controls are frequently associated with the following areas: Chemical, Biotechnology and Biomedical Engineering; Nuclear Technology; Materials Technology; Sensors and Sensor Technology; Remote Sensing, Imaging and Reconnaissance; Advanced Computer/Microelectronic Technology; Navigation, Avionics and Flight Control; Information Security/Encryption; Robotics; Laser and Directed Energy Systems; Rocket Systems; Propulsion System and Unmanned Air Vehicle Subsystems; Marine Technology; Telecommunications/Networking
- http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&sid=9cd3b594bab8f91ce00cb28e9afe7f24&tpl=/ecfrbrowse/Title15/15cfr736_main_02.tpl

International Traffic in Arms Regulations (ITAR)

- International Traffic in Arms Regulations govern the export of defense articles and defense services, i.e. those items with a military application. The licensing conditions for materials covered as military products and technology are set forth at 22 U.S.C. § 2778.

- The munitions list includes such items as firearms, ammunition, explosives, military vehicles, spacecraft, military and space electronics, protective equipment, guidance and control equipment, and some nanotechnology/new materials and sensors. Certain software is also covered. Defense services cover furnishing controlled technical data to foreign nationals anywhere, even if such technical data may be in the public domain.
- http://www.pmdt.state.gov/regulations_laws/itar.html

Non-Disclosure Agreements

- Non-disclosure agreements (NDA), also known as confidentiality agreements, are binding legal contracts that restrict access to proprietary information.

Consulting Contracts

- Consulting contracts are binding legal agreements that contain the terms and conditions by which a client agrees to work with a consultant. Contracts often include the scope of work and payment terms.

Family Educational Rights and Privacy Act (FERPA):

- FERPA protects the privacy of student education records. Generally, schools must have written permission from the student or the parents of a dependent student to release any of the student's education record. It also gives students and parents a right to inspect their education records.
- General Overview: <http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html>
- FAQ: <http://www2.ed.gov/policy/gen/guid/fpco/faq.html#q5>

Colorado Revised Statutes Regarding Student Activity Fees:

- Colorado Revised Statute 23-1-105 contains provisions restricting the use of student activity fees. In general, student fees must be separately accounted for, and student involvement is required in decisions regarding the use of student fees.
- http://www.state.co.us/gov_dir/leg_dir/olls/sl2011a/sl_297.htm

Academic Accreditation

- Accreditation standards ensure that education provided by institutions of higher education meets acceptable levels of quality. The Department of Education provides information on accreditation and accrediting agencies.
- <http://www2.ed.gov/admins/finaid/accred/index.html>

American Recovery and Reinvestment Act of 2009 (ARRA):

- This Act sets forth compliance provisions applicable to entities receiving ARRA monies, including "Buy American", "Wage Rate Requirements" and "Disclosure of Fraud or Misconduct". In addition ARRA requires that certain data elements be reported timely.
- <http://www.ed.gov/recovery>
- http://www.whitehouse.gov/omb/recovery_faqs/

Occupational Health & Safety Act (OSHA):

- OSHA requires that certain precautions be observed and certain actions taken to protect the health and safety of employees on the job. Teachers are considered employees under the act, but students are not covered.
- <http://www.osha.gov>

Environmental Protection Agency (EPA) Laws:

- The Environmental Protection Agency regulates the disposal of hazardous wastes, including wastes from academic laboratories.
- <http://www.epa.gov>

Radioactive Material Regulations:

- To ensure the safe use and disposal of radioactive materials, state and federal regulations govern the possession, use, transport, transfer, and disposal of radioactive material. The purpose of these requirements is to ensure the safe use and disposal of radioactive material.
- <http://www.nrc.gov/>

National Science Foundation Institutional Data Management Requirements

- Grant applications submitted to the National Science Foundation (NSF) will require a maximum two-page supplemental plan for data management and the sharing of research products.
- The NSF's policy on the dissemination and sharing of research results states that: Investigators are expected to share with other researchers, at no more than incremental cost and within a reasonable time, the primary data, samples, physical collections and other supporting materials created or gathered in the course of work under NSF grants. Grantees are expected to encourage and facilitate such sharing.
- <http://www.nsf.gov/bfa/dias/policy/dmpfaqs.jsp#3>

Federal Grant Requirements

- See references in the Research and Administration section

Freedom of Information Act (FOIA) and Colorado Open Records Act (24-72-201, C.R.S.)

- State and federal laws designed to ensure transparency and accountability cover the release of information.
- http://www.justice.gov/oip/foia_updates/Vol_XVII_4/page2.htm

Colorado Open Records Act (Colorado Revised Statute 24-72)

- The Colorado Open Records Act (CORA) is a series of laws designed to guarantee that the public has access to the records of government bodies at all levels in Colorado.
- http://www.state.co.us/gov_dir/leg_dir/olls/colorado_revised_statutes.htm

Human Subjects Research:

- The U.S. Department of Health and Human Services, Office for Human Research Protections, has promulgated regulations to ensure the ethical practice of

research involving human subjects. Research sponsored by other federal agencies and private industry may have additional requirements for human subjects research. Human subjects research regulations are complex and if violations occur, institutions may be subject to a range of penalties, including temporary withholding of payment, repayment of funding, or suspension or disbarment, which disqualifies the institution from receiving federally sponsored grants.

- <http://ohsr.od.nih.gov/guidelines/45cfr46.html>

Animal Research:

- The Animal Welfare Act (AWA) requires that minimum standards of care and treatment be provided for certain animals bred for commercial sale, used in research, transported commercially, or exhibited to the public.
- http://awic.nal.usda.gov/nal_display/index.php?info_center=3&tax_level=3&tax_subject=182&topic_id=1118&level3_id=6735&level4_id=0&level5_id=0&placement_default=0

Drug-Free Schools and Communities Act

- Drug and Alcohol Abuse Prevention Regulations (Education Department General Administrative Regulations [EDGAR]), require that, as a condition of receiving funds or any other form of financial assistance under any federal program, an institution of higher education must certify that it has adopted and implemented a program to prevent the unlawful possession, use, or distribution of illicit drugs and alcohol by students and employees.
- <http://www.higheredcenter.org/mandates/dfsca>

Privacy Act of 1974

- See summary in Links to Key Laws and Regulations – Admissions

Computer Security Act

- See summary in Links to Key Laws and Regulations – Admissions

Post 911/GI Bill Benefits

- See summary in Links to Key Laws and Regulations – Financial Aid

Americans with Disabilities Act

- See summary in Links to Key Laws and Regulations – Human Resources

Constitution Day

- The State of Colorado requires state agencies to celebrate the holiday.

The Solomon Act

- Allows military organizations access to information ordinarily restricted under FERPA for the purpose of military recruiting. For example, the Solomon Amendment allows Department of Defense entities to physically access

- institutional facilities to recruit students, and to obtain students' names, addresses, phone numbers, age, class, and degree program once every term.
- Secondary Source: <http://www.law.georgetown.edu/solomon/solomon.html>

McKinney-Vento Act

- The McKinney Act addresses homeless and disadvantaged youth.
- http://portal.hud.gov/hudportal/HUD?src=/program_offices/comm_planning/homeless/lawsandregs/mckv

Title IX

- See summary in Links to Key Laws and Regulations – Research and Administration

Fair Competition with Private Industry (24-113, 23-41-116, C.R.S.)

- State law prohibits a state agency from engaging in the manufacturing, processing, sale, offering for sale, rental, leasing, delivery, dispensing, distributing, or advertising of goods or services to the public which are also offered by private enterprise unless specifically authorized by law.
- The Board of Trustees is authorized to contract for or impose and collect rents or charges for the use of Colorado School of Mines' buildings and facilities for research, including research conducted by or under the auspices of the Colorado school of mines. Rents or charges must be reasonable, as prescribed.
- http://www.state.co.us/gov_dir/leg_dir/olls/colorado_revised_statutes.htm

Admissions

Family Educational Rights and Privacy Act (FERPA):

- See summary in Links to Key Laws and Regulations – Academic Affairs

The Privacy Act of 1974:

- The Privacy Act requires agencies to ensure the security and confidentiality of records and protect against anticipated threats.
- The Privacy Act of 1974: <http://www.justice.gov/opcl/privstat.htm>
- General Overview: <http://www.hhs.gov/foia/privacy/index.html>

The Computer Security Act:

- The Computer Security Act governs the privacy of sensitive information in Federal computer systems and establishes minimum acceptable security practices.
- <https://www.csp.noaa.gov/policies/csa-1987.htm>

Colorado Higher Education Admissions Requirements (HEAR):

- HEAR sets academic standards for first time freshman applicants and some transfer applicants.
- <http://higher.ed.colorado.gov/Academics/Admissions/default.html>

Discrimination/Sexual Harassment Laws:

- The Office for Civil Rights enforces Federal civil rights laws that prohibit discrimination in programs or activities that receive federal financial assistance from the Department of Education.
- <http://www2.ed.gov/about/offices/list/ocr/aboutocr.html>

Student and Exchange Visitor Program:

- The Student and Exchange Visitor Information System (SEVIS) requires maintenance of status information on foreign students.
- http://www.ice.gov/sevis/schools/new_schools/

Athletics

NCAA/Conference Rules

- NCAA rules govern the conduct of intercollegiate athletics programs of member institutions. Rules include admissions, financial aid, eligibility and recruiting.
- Complete Rulebook:
<http://www.ncaapublications.com/productdownloads/D212.pdf>

Title IX of the Education Amendments of 1972

- Title IX requires that no person, on the basis of sex, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any education program or activity receiving Federal financial assistance, except that:
- <http://www.justice.gov/crt/about/cor/coord/titleixstat.php>
- <http://www.dol.gov/oasam/regs/statutes/titleix.htm>

Tax Laws for Exempt Entities

- To qualify as a tax-exempt entity, a university must limit its activities to the educational purposes for which it was organized and ensure that its assets are dedicated its stated educational purposes. A university must engage primarily in activities that accomplish one or more of its educational missions. A university may carry out its intercollegiate sports program in a tax-exempt manner if the operation of the intercollegiate program is in furtherance of the educational institution's exempt purpose and if the institution is not organized for the primary purpose of carrying on an unrelated trade or business.
- IRS Website: <http://www.irs.gov/charities/index.html?navmenu=menu1>
- Non-primary resource: <http://www.nysscpa.org/taxstringer/2011/feb/roy.htm>

Payment Card Industry (PCI) Standards

- PCI Standards address specifications, tools, measurements and support resources to help organizations ensure the safe handling of cardholder

information. PCI standards include prevention, detection and appropriate reaction to security incidents.

- https://www.pcisecuritystandards.org/security_standards/index.php

NCAA Athletics Certification:

- See NCAA Conference Rules

Americans with Disabilities Act (ADA)

- See summary in Links to Key Laws and Regulations – Human Resources

NCAA Fundraising Regulations

- See NCAA Conference Rules

Finance and Administration

Bond Covenants

- Bond covenants establish the terms and conditions of financing agreements and may include requirements for monitoring bond ratios and debt capacity.

Office of Management and Budget (OMB) Circular A-21

- “Cost Principles for Educational Institutions.” A voluminous and highly complex directive, Circular A-21 sets forth specific compliance requirements for allowable costs, including guidance on 54 selected cost items (training, travel, rent, salaries, meetings, conferences, entertainment, compensation for personal services, etc.).
- http://www.whitehouse.gov/omb/circulars_a021_2004

Procurement Requirements

- Federal and state rules, as well as CSM policies, address such topics as competitive bidding, conflicts of interest, indemnification and capital construction. Laws include:
 - Indemnification (CRS 23-5-106)
 - Purchasing of Furniture (CRS 17-24-111)
 - Capital Construction Statutes
 - http://www.state.co.us/gov_dir/leg_dir/olls/colorado_revised_statutes.htm

Investment Laws & Regulations

- Laws governing investment of public funds place restrictions on which securities public funds may be expended.
- <http://www.e-ccta.org/CCTA/Treas%20Manual/Title24/ManualTitle24Art75.htm>

Internal Audit Standards

- Internal audit standards require the chief audit executive to report to a level within the organization that allows the internal audit activity to fulfill its responsibilities. The chief audit executive must confirm to the board, at least annually, the organizational independence of the internal audit activity.
- <http://www.theiia.org/guidance/standards-and-guidance/>

Foreign Asset Control Regulations

- Foreign asset control regulations address economic and trade sanctions against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States.
- <http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx>

NCAA Athletic Audit Bylaw 22.2.1.2

- Rules compliance program must be evaluated by an authority outside the athletics department.
- See NCAA/Conference rules

The Foreign Corrupt Practices Act of 1977

- The Foreign Corrupt Practices Act makes it unlawful for certain classes of persons and entities to make payments to foreign government officials to assist in obtaining or retaining business.
- <http://www.justice.gov/criminal/fraud/fcpa/>

Freedom of Information Act (FOIA):

- See description in Academic Affairs

Higher Education Act/Higher Education Opportunity Act

- The Higher Ed Act contains reporting requirements for universities. It also addresses campus safety plans and relationships between higher education institutions and student lenders.
- <http://ifap.ed.gov/dpccletters/attachments/GEN0812FP0810AttachHEOADCL.pdf>
- http://www.edfund.org/pdfs/HEOA_Overview.pdf
- Section 488, Missing Student Policy requires any institution participating in a Title IV federal student financial aid program that maintains on campus housing facilities to establish a missing student notification policy and related procedures for those students who live in on campus housing and who have been missing for 24 hours.
- Fire safety reporting requirements for institutions with on-campus student housing facilities
- <http://www2.ed.gov/admins/lead/safety/handbook-2.pdf>
- The University must post student transfer policies.

- Publishers must disclose textbook price and revision information to faculty during the marketing process.
- Complete Act: <http://www.nacua.org/documents/heoa.pdf>

Federal and State Tax Laws

- The University must comply with both the Federal Internal Revenue Code and the Colorado Revised Statutes regarding taxes. In particular, efforts should be taken to ensure tax-exempt status is maintained. All reports need to be filed timely and in accordance with IRS procedures.
- <http://www.irs.gov/index.html>
- Tax Exempt Compliance Project:
<http://www.irs.gov/charities/article/0,,id=186865,00.html>

Fair and Accurate Credit Transactions – Red Flag Rules

- Red Flags Rules require implementation of a written Identity Theft Prevention Program designed to detect the warning signs — or "red flags" — of identity theft in their day-to-day operations.
- Requires financial institutions or creditors to develop and implement an Identity Theft Prevention Program in connection with both new and existing accounts. The Program must include reasonable policies and procedures for detecting, preventing, and mitigating identity theft.
- http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ159.108.pdf
- <http://www.ftc.gov/bcp/edu/microsites/redflagsrule/index.shtml>

Donor Terms

- See complete description and risk evaluation in Key Risk Areas – Donations.

Revised Federal Sentencing Guidelines for Organizations (FSGO)

- Each organization is responsible for the wrongful acts of its employees as long as they employees were acting in their official capacity. The theory is that each organization shares a degree of culpability if an employee acts in an unlawful manner, even if the organization did not know of or approve of their actions. Federal prosecutions of organizations frequently involve individual and organizational defendants.
- [http://www.ussc.gov/Guidelines/Organizational Guidelines/guidelines_chapter_8.htm](http://www.ussc.gov/Guidelines/Organizational%20Guidelines/guidelines_chapter_8.htm)

Lobbying and Disclosure Act

- Under federal law, an individual retained by the University for services that include more than one "lobbying contact" and whose "lobbying activities" for the University constitute twenty percent or more of his or her work time over a six-month period is a "lobbyist." The University must register its lobbyists as required by the federal Lobbying Disclosure Act of 1995, and all registered lobbyists are required to submit a report every six months containing specific

information concerning their lobbying activities, including the issues lobbied upon, officials contacted, time spent, and an estimate of expenses.

- <http://lobbyingdisclosure.house.gov/>
- http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ65.104.pdf

40CFR31.36: Utilization of Women Owned Businesses (E.O. 12138), Utilization of Minority Owned Businesses (E.O. 11625), Small and Disadvantaged Businesses

- The head of each Federal department and agency, or a representative designated by him, when and in the manner so requested by the Secretary shall furnish information, assistance, and reports to, and shall otherwise cooperate with, the Secretary in the performance of his functions hereunder.
- Each Federal department or agency shall, within constraints of law and appropriations therefore, continue all current efforts to foster and promote minority business enterprises and to support the program herein set forth, and shall cooperate with the Secretary of Commerce in increasing the total Federal effort.
- <http://www.archives.gov/federal-register/codification/executive-order/11625.html>

Non-Delinquency on Federal Debt

- OMB Circular A-129 provides requirements for managing Federal credit programs and for collecting non-tax receivables. It sets principles for designing credit programs, including: the preparation and review of legislation and regulations; budgeting for the costs of credit programs and minimizing unintended costs to the Government; and improving the efficiency and effectiveness of Federal credit programs. It also sets standards for extending credit, managing lenders participating in Government guaranteed loan programs, servicing credit and non-tax receivables, and collecting delinquent debt.
- http://www.whitehouse.gov/omb/circulars_a129rev/

Financial Aid

Pell Grants/Federal Aid

- The Federal Pell Grant Program provides need-based grants to low-income undergraduate and certain post baccalaureate students to promote access to postsecondary education. Universities are required to properly account for the Pell Grants and provide program refunds in certain instances.
- <http://www2.ed.gov/programs/fpg/index.html>
- <https://studentaid.ed.gov/PORTALSWebApp/students/english/PellGrants.jsp?tab=funding>

Free Application for Federal Student Aid

- The Free Application for Federal Student Aid (FAFSA) is the form the U.S. Department of Education (ED) requires to determine a student's Expected

- Family Contribution (EFC). The government conducts a “need analysis” based on financial information, such as income, assets, and other family information, which the student will be asked to provide.
- The University is required to ensure it only gives awards to students that are eligible based on admittance, enrollment, grade level, and need. Awards can only be made after a FAFSA is verified.
 - <http://www.fafsa.com/>

Donor Scholarships

- The School of Mines Foundation, an independent tax-exempt entity founded in 1928 and incorporated in 1951, is the official gift-receiving agency for the institution. The Foundation works with the financial aid office to provide designated scholarship funds. The financial aid office is required to meet the requirements in the donor agreement.

Federal Work Study Regulations

- A school must make FWS jobs reasonably available to all eligible students at the school. To the maximum extent practicable, a school must provide FWS jobs that complement and reinforce each recipient’s educational program or career goals. In assigning an FWS job, a school must consider the student’s financial need, the number of hours per week the student can work, the period of employment, the anticipated wage rate, and the amount of other assistance available to the student. While there is no minimum or maximum award, the amount for each student should be determined based on these factors.
- FWS employment must be governed by employment conditions, including pay, that are appropriate and reasonable according to the type of work performed, the geographic region, the employee’s proficiency, and any applicable federal, state, or local law.
- <http://www.ifap.ed.gov/sfahandbooks/attachments/0607Vol6Ch2OperatingFWS.pdf>

Federal/State Financial Aid Regulations

- Financial aid regulations require universities to comply with Title IV of the Higher Education Act, and complete the Federal Fiscal Operations Report and Application to Participate (FISAP) and the Colorado Student Unit Record Data System (SURDS).
- Information for Financial Aid Professionals: <http://www.ifap.ed.gov/ifap/>
- FISAP forms: <https://cbfisap.ed.gov/ecb/CBSWebApp/>
- Colorado SURDS: <https://surds.colorado.gov/>

Family Educational Rights and Privacy Act

- See summary in Links to Key Laws and Regulations - Academic Affairs

Privacy Act of 1974

- See summary in Links to Key Laws and Regulations – Admissions

Computer Security Act

- See summary in Links to Key Laws and Regulations – Admissions

Post 911/GI Bill

- The Post-9/11 GI Bill offers benefits for service members and veterans attending education and training programs taken at accredited colleges or universities.
- <http://www.military.com/education/content/gi-bill/new-post-911-gi-bill-overview.html>

Department of Veteran’s Affairs Financial Aid

- The U.S. Department of Veterans Affairs establishes requirements for approved programs of education or training for eligible students. An approved program is a course of study or a program of training that the appropriate state approving agency has determined meets the legal requirements for payment of DVA educational assistance benefits to veterans and other eligible persons. Universities are required to work with the U.S. Department of Veterans Affairs to certify students.
- VA education benefits may be authorized for veterans and qualified dependents under specific chapters of Title 38, U.S. Code (USC). Each VA education program has distinct eligibility requirements.
- <http://www.gibill.va.gov/school%2Dcertifying%2Dofficials/>

Fair and Accurate Credit Transactions Act – Red Flag Rules

- See summary in Links to Key Laws and Regulations – Finance and Administration

College Opportunity Fund

- The College Opportunity Trust Fund (COF), created by the Colorado Legislature, provides a stipend to eligible undergraduate students. The stipend pays a portion of total in-state tuition.
- <https://cof.college-assist.org/COFApp/COFApp/Default.aspx>

Title IV of the Higher Education Act

- Title IV establishes rules for the administration of financial aid. According to federal regulations, colleges and universities that administer federal Title IV funds must disclose certain information to prospective and enrolled students, parents and employees, including information about academic programs, graduation and completion rates, and crime statistics.
- http://federalstudentaid.ed.gov/about/title4_programs.html

Graduate Studies

Export Administration Regulations

- See summary in Links to Key Laws and Regulations – Academic Affairs

Non-Disclosure Agreement Requirements

- See summary in Links to Key Laws and Regulations – Academic Affairs

Residency Requirements

- Colorado law (23-7-101, C.R.S. et seq) requires state institutions of higher education to apply uniform rules to determine whether students should be classified as in-state students or out-of-state students for tuition purposes.
- <http://higher.ed.colorado.gov/Finance/Residency/statutes.html>

America Competes Act

- Under America Competes any institution that applies for financial assistance from the National Science Foundation must describe in its grant proposal a plan to provide appropriate training and oversight in the responsible and ethical conduct of research to undergraduate students, graduate students, and postdoctoral researchers participating in the proposed research project.
- The institution is responsible for certification that a Responsible Conduct of Research (RCR) training plan is in place and verification that the students and post docs have completed RCR training. This certification must be in place at the time of proposal submission. Training plans do not need to be submitted with the proposal, but are subject to review upon request.
- <http://www.nsf.gov/bfa/dias/policy/rcr.jsp>
- http://www.nsf.gov/pubs/policydocs/rcr/faqs_mar10.pdf

Privacy Act of 1974

- See summary in Links to Key Laws and Regulations – Admissions

Family Educational Rights and Privacy Act

- See summary in Links to Key Laws and Regulations – Admissions

Human Subjects Research

- See summary in Links to Key Laws and Regulations – Academic Affairs

Federal Grants/Sponsored Research

- See summary and risk description in Key Risks – Federal Grants

Work Study Regulations

- See summary in Links to Key Laws and Regulations – Financial Aid

Human Resources

Immigration and Nationality Act

- The Immigration and Nationality Act (INA) sets forth the conditions for the temporary and permanent employment of aliens in the United States and includes provisions that address employment eligibility and employment verification. These provisions apply to all employers.

- <http://www.dol.gov/compliance/laws/comp-ina.htm>

Office of Foreign Assets Control (OFAC)

- See summary in Links to Key Laws and Regulations – Finance and Administration

Health Insurance Portability and Accountability (HIPAA)

- See summary in Links to Key Laws and Regulations – Student Life

The Uniformed Services Employment and Reemployment Rights Act of 1994 (USERRA)

- USERRA establishes the cumulative length of time that an individual may be absent from work for military duty and retain reemployment rights to five years.
- USERRA provides protection for disabled veterans, requiring employers to make reasonable efforts to accommodate the disability. Service members convalescing from injuries received during service or training may have up to two years from the date of completion of service to return to their jobs or apply for reemployment.
- <http://www.dol.gov/vets/programs/userra>

Emergency Preparedness and Disaster Recovery – Clery Act

- See summary in Links to Key Laws and Regulations – Student Life

Executive Order 11246/Office of Federal Contract Compliance Programs

- Executive Order 11246 prohibits federal contractors and federally-assisted construction contractors and subcontractors, who do over \$10,000 in Government business in one year from discriminating in employment decisions on the basis of race, color, religion, sex, or national origin. The Executive Order also requires Government contractors to take affirmative action to ensure that equal opportunity is provided in all aspects of their employment.
- <http://www.dol.gov/compliance/laws/comp-eeo.htm>

IRS Requirements for Benefits Plans

- Among other requirements, the IRS mandates universal availability and written plan rules for 403(b) plans.
- The Universal Availability rule states that if any employee is permitted to make elective salary deferrals to a 403(b) plan, then all employees (with few exceptions), must be allowed the same opportunity.
- <http://www.irs.gov/retirement/index.html>
- http://www.nacubo.org/Business_and_Policy_Areas/Tax/Tax_News/IRS_Announcements_403%28b%29_Employee_Retirement_Plan_Compliance_Project.html

Executive Order 13166

- Executive Order 13166 requires federal agencies to examine the services they provide, identify any need for services to those with limited English proficiency (LEP), and develop and implement a system to provide those services so LEP persons can have meaningful access to them.

- <http://www.justice.gov/crt/about/cor/Pubs/eolep.php>

Fair Labor Standards Act (FLSA)

- FLSA prescribes standards for the basic minimum wage and overtime pay. The Act requires employers to pay covered employees who are not otherwise exempt at least the federal minimum wage and overtime pay of one-and-one-half-times the regular rate of pay.
- FLSA requires employers to prominently post various notices pertaining to specific requirements of the Act in the workplace. The poster that specifically addresses the concerns of young workers is the "Minimum Wage Poster," which states the allowable work hours and times for employees under the age of 18.
<http://www.dol.gov/compliance/laws/comp-flsa.htm>

Consolidated Omnibus Budget Reconciliation Act (COBRA)

- COBRA establishes requirements for continuation of group health coverage that otherwise might be terminated.
- http://www.dol.gov/ebsa/faqs/faq_compliance_cobra.html

Family and Medical Leave Act (FMLA)

- FMLA entitles eligible employees of covered employers to take unpaid, job-protected leave for specified family and medical reasons with continuation of group health insurance coverage under the same terms and conditions as if the employee had not taken leave.
- <http://www.dol.gov/whd/fmla/>

The Americans with Disabilities Act (ADA)

- ADA makes it illegal to discriminate against a qualified person with a disability. The law also requires that employers reasonably accommodate the known physical or mental limitations of an otherwise qualified individual with a disability who is an applicant or employee, unless doing so would impose an undue hardship on the operation of the employer's business.
- http://www.eeoc.gov/laws/statutes/adaaa_info.cfm

Genetic Information Nondiscrimination Act (GINA)

- GINA provides protection against discrimination based on genetic information in the health insurance and employment areas.
- <http://www.genome.gov/24519851>

Code of Federal Regulations Title 34 – Student Assistance Provisions

- Title 34 establishes general rules that apply to an institution that participates in any student financial assistance program authorized by Title IV of the Higher Education Act of 1965, as amended (Title IV, HEA program).
- <http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr;rgn=div5;view=text;node=34%3A3.1.3.1.34;idno=34;sid=83816ab6ebedaa009e6e6cb6ae3a21bf;cc=ecfr>

Patient Protection and Affordable Care Act

- The Patient Protection and Affordable Care Act provides requirements regarding access to quality, affordable health care.
- <http://www.dol.gov/ebsa/healthreform/>
- <http://dpc.senate.gov/healthreformbill/healthbill04.pdf>

Fair Credit Reporting Act

- The Fair Credit Reporting Act regulates the collection, dissemination, and use of consumer information, including consumer credit information. Along with the Fair Debt Collection Practices Act (FDCPA), it forms the base of consumer credit rights in the United States.
- <http://www.ftc.gov/os/statutes/031224fcra.pdf>

Workers Compensation

- Administered by the Department of Labor, workers compensation covers employees injured at work or who acquire an occupational disease.
- <http://www.dol.gov/dol/topic/workcomp/index.htm>

Equal Employment Opportunity Act

- Equal opportunity laws guard against workplace discrimination based on an individual's race, color, national origin, religion, sex, age, perceived intelligence, or disability. Laws prohibit retaliation for reporting and/or opposing a discriminatory practice.
- <http://www.eeoc.gov/>

Title VII of the Civil Rights Act of 1964 (Title VII)

- Title VII prohibits harassment and discrimination on the basis of race, color, religion, national origin, or sex.
- <http://www.eeoc.gov/laws/statutes/titlevii.cfm>

The Equal Pay Act of 1963 (EPA)

- EPA makes it illegal to pay different wages to men and women if they perform equal work in the same workplace.
- <http://www.eeoc.gov/laws/statutes/epa.cfm>

The Age Discrimination in Employment Act of 1967 (ADEA)

- Protects people who are 40 or older from discrimination because of age.
- <http://www.eeoc.gov/laws/statutes/adea.cfm>

Information Technology

Digital Millennium Copyright Act

- The Digital Millennium Copyright Act amended the United States Copyright Act, Title 17 of the U.S. Code, to provide certain limitations on the liability of online service providers (OSPs) for copyright infringement.

- <http://www.copyright.gov/legislation/dmca.pdf>

Intellectual Property Laws

- Intellectual property laws require universities to protect their own intellectual property, including research data and avoid infringement on others intellectual property, including software and media.
- <http://www.uspto.gov/ip/global/index.jsp>

Payment Card Industry (PCI) Security Requirements

- See summary in Links to Key Laws and Regulations – Athletics

Mobile Device Security

- NSF requires all proposals to describe plans for data management and sharing of products of research, or assert the absence of need for such plans.
- Mobile devices must comply with the data security requirements in HIPAA, FERPA, the Computer Security Act, and other laws previously mentioned.
- <http://www.nsf.gov/bfa/dias/policy/dmp.jsp>

Record Retention Laws

- Federal records may not be destroyed-except in accordance with the procedures described in [Chapter 33 of Title 44](#), United States Code.
- <http://www2.ed.gov/policy/gen/leg/fra.html>

Health Insurance Portability and Accountability (HIPAA)

- See summary in Links to Key Laws and Regulations – Student Life

Family Educational Rights and Privacy Act

- See summary in Links to Key Laws and Regulations – Admissions

Privacy Act of 1974

- See summary in Links to Key Laws and Regulations – Admissions

NSF Data Requirements

- All proposals must describe plans for data management and sharing of the products of research, or assert the absence of the need for such plans. FastLane will not permit submission of a proposal that is missing a Data Management Plan. The Data Management Plan will be reviewed as part of the intellectual merit or broader impacts of the proposal, or both, as appropriate.
- <http://www.nsf.gov/eng/general/dmp.jsp>

Computer Security Act

- See summary in Links to Key Laws and Regulations – Admissions

State Notification Laws Colorado Revised Statute (6-1-716, C.R.S.)

- State laws require notification of a breach of the security of personal information and a prompt investigation to determine the likelihood that personal information has been or will be misused.
- <http://www.michie.com/colorado/lpext.dll?f=templates&fn=main-h.htm&cp=>

Americans with Disabilities Act

- See summary in Links to Key Laws and Regulations – Athletics

Federal Rules of Civil Procedure

- Federal rules govern the retention and protection of electronically stored information. Colleges and universities that do not actively manage their Electronically Stored Information (ESI) may face difficulties in compliance, increased risks of sanctions, and higher litigation costs.
- <http://www.educause.edu/EDUCAUSE+Review/EDUCAUSEReviewMagazineVolume42/ElectronicallyStoredInformation/158139>

Higher Education Act/Higher Education Opportunity Act

- See summary in Links to Key Laws and Regulations – Finance and Administration

Gramm-Leach-Bliley Act

- The Gramm-Leach-Bliley Act requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.
- <http://business.ftc.gov/privacy-and-security/gramm-leach-bliley-act>

Computer Assistance for Law Enforcement Act (CALEA)

- CALEA requires telecommunications carriers to assist law enforcement in executing electronic surveillance pursuant to court order or other lawful authorization.
- <http://www.justice.gov/criminal/cybercrime/searching.html>
- <http://www.askcalea.net/>

Plant Operations

Procurement – Contracting Rules

- General Rules: See summary in Links to Key Laws and Regulations – Finance and Administration
- Minority Owned Businesses: See summary in Links to Key Laws and Regulations – Finance and Administration

Fire Codes

- The Fire Marshal's Office is responsible for managing the University's compliance with the State Fire Prevention Code and other applicable fire safety laws and standards; providing fire safety education and training; investigating all fires that occur on University property; and performing plan review and construction inspections. Fire Marshals are delegated fire prevention and investigation authority by the Colorado State Fire Marshal.
- <http://dfs.state.co.us/>

Occupational Safety & Health Act (OSHA)

- OSHA governs safety in the workplace. Regulations cover many activities in colleges and universities. Although OSHA regulations were written specifically for employees, they provide a good framework for creating a safe working environment free of recognizable hazards. Most of the programs in the health and safety guide extend to faculty, staff, undergraduates, and graduates.
<http://www.osha.gov/>
- Chemical Safety: OSHA provides a standard for occupational exposure to hazardous chemicals in laboratories- "Laboratory Standard". Under this standard, a laboratory is required to produce a Chemical Hygiene Plan that addresses the specific hazards found in its location.
<http://www.osha.gov/SLTC/laboratories/index.html>
- Compressed Gasses: "Inspection of compressed gas cylinders" requires compressed gas cylinders to be in a safe condition to the extent that this can be determined by visual inspection. Visual and other inspections must be conducted as prescribed in the Hazardous Materials Regulations of the Department of Transportation (49 CFR parts 171-179 and 14 CFR part 103). Where those regulations are not applicable, visual and other inspections must be conducted in accordance with Compressed Gas Association Pamphlets C-6-1968 and C-8-1962, which is incorporated by reference as specified in Sec. 1910.6.
http://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=STANDARDS&p_id=9747

Critical Building Codes

- HVAC:
 - The national consensus standard for outside air ventilation is ASHRAE Standard 62.1-200, Ventilation for Acceptable Indoor Air Quality and its published Addenda. This standard specifies the amount of outside air that must be provided by natural or mechanical ventilation systems to various areas of the school, including classrooms, gymnasiums, kitchens and other special use areas.
 - <http://www.ashrae.org/technology/page/548>
- Elevators/Lifts: An installation permit is required prior to commencement of work for an installation of a new regulated lifting device. An alteration permit is required prior to commencement of work for an alteration to an existing regulated lifting device.
 - www.in.gov/legislative/iac/T06750/A00210.PDF

Colorado Department of Public Health and Environment (CDPHE) - Swimming Pool Maintenance

- CDPHE requires natural swimming areas to have an approved management plan.
- <http://www.cdphe.state.co.us/regulations/waterqualitycontroldivision/index.html>

Federal and State Construction Statutes

- The State Buildings Program (SBP) establishes minimum building codes for all construction by state agencies on state-owned or state lease-purchased properties or facilities.
- <http://www.colorado.gov/cs/Satellite/DPA-EO/DEO/1251570153250>

Environmental Protection Agency Laws

- The EPA has primary responsibility for enforcing many of the environmental statutes and regulations of the United States. As such, the Agency is granted explicit enforcement authority in environmental statutes.
- <http://www.epa.gov/>
- Examples of EPA regulations include:
 - Resource Conservation and Recovery Act: The Resource Conservation and Recovery Act (RCRA) gives the EPA the authority to control hazardous waste from the "cradle-to-grave." This includes the generation, transportation, treatment, storage, and disposal of hazardous waste. RCRA also set forth a framework for the management of non-hazardous solid wastes.
 - <http://www.epa.gov/lawsregs/laws/rcra.html>
 - Comprehensive Environmental Response, Compensation, and Liability Act: The Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA), commonly known as Superfund, addresses Federal response to releases or threatened releases of hazardous substances that may endanger public health or the environment. <http://www.epa.gov/superfund/policy/cercla.htm>
 - Nanomaterials: Many nanoscale materials are regarded as "chemical substances" under the Toxic Substances Control Act (TSCA). <http://www.epa.gov/oppt/nano/>
 - Asbestos: See regulations at: <http://www.epa.gov/asbestos/>

City of Golden Water Permits

- Local regulations govern water permits.
- <http://www.cityofgolden.net/government/departments-divisions/water/utilities/>

Colorado Department of Health Regulations

- The Colorado Department of Health is responsible for a variety of areas that potentially affect the health of Colorado's people and the quality of its

environment. The Department creates and enforces regulations regarding solid and hazardous waste, hazardous materials, health facilities, and laboratories.

- <http://www.cdphe.state.co.us/>

Americans with Disabilities Act

- See summary in Links to Key Laws and Regulations - Athletics

Equipment Safety Including Vehicles

- Colorado School of Mines Facilities Management is responsible for overseeing the procurement, licensing, maintenance, repair, records maintenance and disposal of Mines vehicles. This policy is applicable to the entire Mines fleet, which includes department vehicles.
- http://inside.mines.edu/UserFiles/File/policies/FPS/FM_Vehicle_Fleet_Policy.pdf

Chemical/Hazardous Waste Regulations

- Chemical Facility Anti-Terrorism Standards (CFATS)
 - Appendix A of the Chemical Facility Anti-Terrorism Standards (CFATS) regulation lists the DHS chemicals of interest and their corresponding Screening Threshold Quantities (STQ). If a facility possesses, or later comes into possession, of a chemical of interest at or above the specified screening threshold quantity, that facility must complete an online consequence assessment tool, known as a Top-Screen.
 - Colleges and universities that meet the Appendix A levels – that is, those that possess Appendix A chemicals of interest at or above the listed screening threshold quantities – will have to complete and submit a Top-Screen to DHS.
 - http://www.dhs.gov/files/laws/gc_1166796969417.shtm
 - http://www.dhs.gov/xlibrary/assets/IP_ChemicalFacilitySecurity.pdf
 - http://www.dhs.gov/xnews/releases/pr_1193971455405.shtm
- OSHA: In order to ensure chemical safety in the workplace, information must be available about the identities and hazards of the chemicals. OSHA's Hazard Communication Standard (HCS) requires the development and dissemination of such information. <http://www.osha.gov/dsg/hazcom/index.html>
- EPA: The Chemical Safety Information, Site Security and Fuels Regulatory Relief Act establishes amended provisions for reporting and disseminating information under Section 112(r) of the Clean Air Act.
 - <http://www.epa.gov/OEM/content/lawsregs/chemover.htm>
 - <http://www.epa.gov/ceppo/pubs/title3.pdf>

Radiation Safety Regulations

- 10 CFR 20: Standards for Protection Against Radiation
 - Regulations establish standards for protection against radiation and control the receipt, possession, use, transfer, and disposal of licensed material.

- <http://www.nrc.gov/reading-rm/doc-collections/cfr/part020/part020-1001.html>
- EPA Laws regarding radiation: <http://www.epa.gov/rpdweb00/>

Suppliers Compliance with Laws & Regulations

- The University must monitor supplier compliance with laws and regulations.

Research and Administration

Federal Grant Requirements/Grant Financial Compliance

- Office of Management and Budget (OMB) Circular A-110 Uniform Administrative Requirements for Grants and Agreements with Institutions of Higher Education, Hospitals, and Other Non-Profit Organizations” addresses critical compliance areas such as reporting, procurement, property management, codes of conduct (including conflicts of interest), audits and cost sharing arrangements.
 - http://www.whitehouse.gov/omb/circulars_a110
- Office of Management and Budget (OMB) Circular A-21:
 - “Cost Principles for Educational Institutions.” A voluminous and highly complex directive, Circular A-21 sets forth specific compliance requirements for allowable costs, including guidance on 54 selected cost items (training, travel, rent, salaries, meetings, conferences, entertainment, compensation for personal services, etc.).
 - http://www.whitehouse.gov/omb/circulars_a021_2004

Sub-Recipient Monitoring

- Office of Management and Budget (OMB) Circular A-133:
 - Circular A-133 sets forth standards for obtaining consistency and uniformity among Federal agencies for the audit of non-Federal entities expending Federal awards, including sub-recipient monitoring. Other circulars and laws (A-129 and the Cash Management Act describe requirements for managing cash drawdowns and ensuring non-delinquency.
 - <http://www.whitehouse.gov/sites/default/files/omb/circulars/a133/a133.pdf>
- The University must have a formal process that would provide risk assessments on sub-awardees on an on-going basis at the post-subaward stage and provide monitoring activities on the subawardees. It must also document the results of a risk assessment on potential subawardees at the pre-subaward stage. <http://www.nsf.gov/pubs/gpg/faqs.pdf>

Bayh-Dole Act

- See summary in Links to Key Laws and Regulations – Technology Transfer

Foreign Corrupt Practices Act

- See summary in Links to Key Laws and Regulations – Finance and Administration

Export Administration Regulations

- See summary in Links to Key Laws and Regulations – Academic Affairs

Private Use of State Property/Protection of University Assets (5 C.F.R. 2635.101)

- Requires employees to safeguard federal property and use it only for authorized activities.
- This law is particularly important in the realm of external consulting contracts. Faculty must be aware of the laws and either avoid use or compensate the university for any use of labs/classrooms/research facilities.
- http://www.dod.gov/dodgc/defense_ethics/resource_library/2010_Deskbook/8ECC_UseOfGovernmentResources.pdf

Title IX

- Title IX of the Education Amendments of 1972 prohibits discrimination on the basis of sex, requiring that "no person in the United States shall, on the basis of sex, be excluded from participation in, be denied the benefits of, or be subjected to discrimination under any education program or activity receiving Federal financial assistance." Title IX has broad applicability.
- <http://www.dol.gov/oasam/regs/statutes/titleix.htm>

External Consulting Contracts/Industry Contracts

- See summary in Key Risk Areas – Professional Consulting Contracts

Human Subjects Research

- See summary in Links to Key Laws and Regulations – Academic Affairs

Non-Disclosure Agreements

- See summary in Links to Key Laws and Regulations – Academic Affairs

National Science Foundation (NSF) Requirements

- The NSF has several requirements of institutions that receive funding. Below is a description of the major areas. For a complete review of requirements, visit the NSF website: <http://www.nsf.gov/bfa/dias/policy/>
- Responsible Conduct of Research: "The Director shall require that each institution that applies for financial assistance from the Foundation for science and engineering research or education describe in its grant proposal a plan to provide appropriate training and oversight in the responsible and ethical conduct of research to undergraduate students, graduate students, and postdoctoral researchers participating in the proposed research project."
<http://www.nsf.gov/bfa/dias/policy/rcr.jsp>
- Data Management Requirements: Proposals submitted or due on or after January 18, 2011, must include a supplementary document of no more than two pages labeled "Data Management Plan". This supplementary document should describe how the proposal will conform to NSF policy on the dissemination and

- sharing of research results. See [Grant Proposal Guide \(GPG\) Chapter II.C.2.j](#) for full policy implementation. <http://www.nsf.gov/bfa/dias/policy/dmp.jsp>
- Cost Sharing is required for proposals submitted, and awards made, in response to NSF programs. Such cost sharing must meet the definition of cost sharing as specified in 2 CFR 215 (OMB Circular A-110) and will be auditable. <http://www.nsf.gov/bfa/dias/policy/csdocs/principles.pdf>
 - Research Performance Progress Reports: A specified reporting format for grant reporting progress. <http://www.nsf.gov/bfa/dias/policy/rppr/policyletter.pdf>

Strategic Operations

Continuing Education Contracts

- The University has a variety of continuing education contracts. Violation of these contracts could result in potential lawsuits for the University. The terms of these contracts vary and need to be reviewed on an individual basis.

Export Administration Regulations

- See summary in Links to Key Laws and Regulations – Academic Affairs

International Traffic in Arms Regulations

- See summary in Links to Key Laws and Regulations – Academic Affairs

Foreign Corrupt Practices Act

- See summary in Links to Key Laws and Regulations – Finance and Administration

Student Life

Fair Housing Statutes

- Colorado's Fair Housing statutes prohibit discrimination with regard to renting or purchasing housing based on race, color, religion, creed, sex, national origin, ancestry, familial status, sexual orientation, marital status or disability.
- http://www.dora.state.co.us/dora_pages/topicarchive/FairHousing.html

Americans with Disabilities Act (ADA)

- See summary in Links to Key Laws and Regulations – Human Resources

Housing Contracts

- The University must abide by state housing laws. Colorado Revised Statutes Title 38, Article 12 details the responsibilities of both landlords and tenants.
- http://www.state.co.us/gov_dir/leg_dir/olls/colorado_revised_statutes.htm
- <http://portal.hud.gov/hudportal/HUD?src=/states/colorado/renting/tenantrights>

Student and Exchange Visitor Program (SEVP)

- See summary in Links to Key Laws and Regulations – Admissions

Family Educational Rights and Privacy Act

- See summary in Links to Key Laws and Regulations – Admissions

The Privacy Act of 1974

- See summary in Links to Key Laws and Regulations – Admissions

The Computer Security Act

- See summary in Links to Key Laws and Regulations – Admissions

Contractor Compliance

- Contractors must maintain approved employment practices and submit any requested compliance reports. Prime or general contractors have the responsibility to ensure that their subcontractors file the proper reports.
- The University should review worker employment status to ensure they are properly classified as either employees or independent contractors.
- Secondary Source: <http://independentcontractorcompliance.com/legal-resources/federal-government-state-task-force-and-university-reports/>

Professional Counseling Licensure/Student Counseling Confidentiality/12-43-101, C.R.S. et seq)

- Professional counseling statutes provide for protection of client information. Confidentiality may be broken only in cases of emergency or legal requirement.
- C.R.S. 12-43-101 states the requirements for professional counseling licensure.
- <http://www.dora.state.co.us/mental-health/>
- <http://www.dora.state.co.us/mental-health/lpc/lpcrules.pdf>

Health and Fire Codes in the Dining Facilities

- See summary in Links to Key Laws and Regulations – Plant Operations

Health Insurance Portability and Accountability (HIPAA)

- HIPAA protects all "individually identifiable health information" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. Covered entities, such as CSM's health clinics, health plans, and mental health clinics, may not disclose protected health information without the individual's written authorization. Non-willful violations of HIPAA may subject the institution to civil financial penalties; willful violations may subject an entity to both civil and criminal penalties.
- <http://www.hhs.gov/ocr/privacy/>

Health Services Licensing

- State law specifies the types of health care entities that must be licensed prior to providing services in the State. The Health Facilities and Emergency Medical

Services Division (hereinafter "Division") inspects health care entities for compliance with regulatory and statutory requirements for state licensure and Medicare/Medicaid certification.

- <http://www.cdphe.state.co.us/hf/>
- http://www.cdphe.state.co.us/hf/lic_cert.pdf

Clery Act - Emergency Preparedness and Disaster Recovery

- The *Jeanne Clery Disclosure of Campus Security Policy and Campus Crime Statistics Act (Clery Act)* is a federal mandate requiring all institutions of higher education (IHEs) that participate in the federal student financial aid program to disclose information about crime on their campuses and in the surrounding communities. Campuses that fail to comply with the act can be penalized with large fines and may be suspended from participating in the federal financial aid program.
- <http://www2.ed.gov/admins/lead/safety/campus.html>
- <http://www.higheredcenter.org/mandates/clery-act>

Export Administration Regulations

- See summary in Links to Key Laws and Regulations – Academic Affairs

Occupational Safety and Health laws

- See summary in Links to Key Laws and Regulations – Academic Affairs

State Health Insurance Provider Laws

- The University has the right to determine what is required for health and safety on a campus and has elected to require institutionally provided health insurance.
- The Colorado Division of Insurance regulates the insurance industry and assists consumers and other stakeholders with insurance issues.
<http://www.dora.state.co.us/insurance/>

Technology Transfer

Bayh-Dole Act

- As a result of this law, universities retain ownership to inventions made under federally funded research. In return, universities are expected to file for patent protection and to ensure commercialization upon licensing. The royalties from such ventures are shared with the inventors; a portion is provided to the University and department/college; and the remainder is used to support the technology transfer process
- <https://s-edison.info.nih.gov/iEdison/>
- http://www.csurf.org/enews/bayhdole_403.html

Export Administration Regulations

- See summary in Links to Key Laws and Regulations – Academic Affairs

Patent Accounting

- School policy is written in accordance with Federal and State Laws:
- Net proceeds from the item of Intellectual Property is calculated by subtracting the costs of obtaining and maintaining a patent that are not reimbursed by the party(s) licensing the technology, if any, and all other expenses of commercial exploitation from the gross proceeds. These expenses shall first be returned to CSM prior to any further distribution of proceeds from the Intellectual Property.
- Of the first thirty thousand dollars (\$30,000) in net proceeds (excluding reimbursement for patent costs), fifteen thousand (\$15,000) will be distributed to the Inventor(s) and fifteen thousand (\$15,000) to the Office of Research and Technology Transfer for investment in speculative patents.
- After the initial thirty thousand (\$30,000) of net proceeds, any additional revenue will be divided as follows: 35% to the Inventor(s); 35% to the CSM general fund and 30% to either the CSM academic department that is the home department(s) of the Inventor(s) or the research center which funded the research, at the discretion of the Inventor(s).

External Consulting Contracts

- School policy dictates that the University owns an invention that is created/developed under the time or resources of the School.
- See more information in Key Risk Areas – Professional Consulting Contracts

Federal and State Tax Laws

- Patents need to be accounted for as intangible assets:
<http://www.irs.gov/pub/irs-pdf/p551.pdf>

University Advancement

Donor Terms and Conditions – Scholarships/Donation Terms on Restricted Endowments

- The University must comply with specific restrictions established by donors.

Federal and State Reporting Requirements

- Federal and State reporting requirements govern nonprofit entities.
- <http://www.irs.gov/charities/>