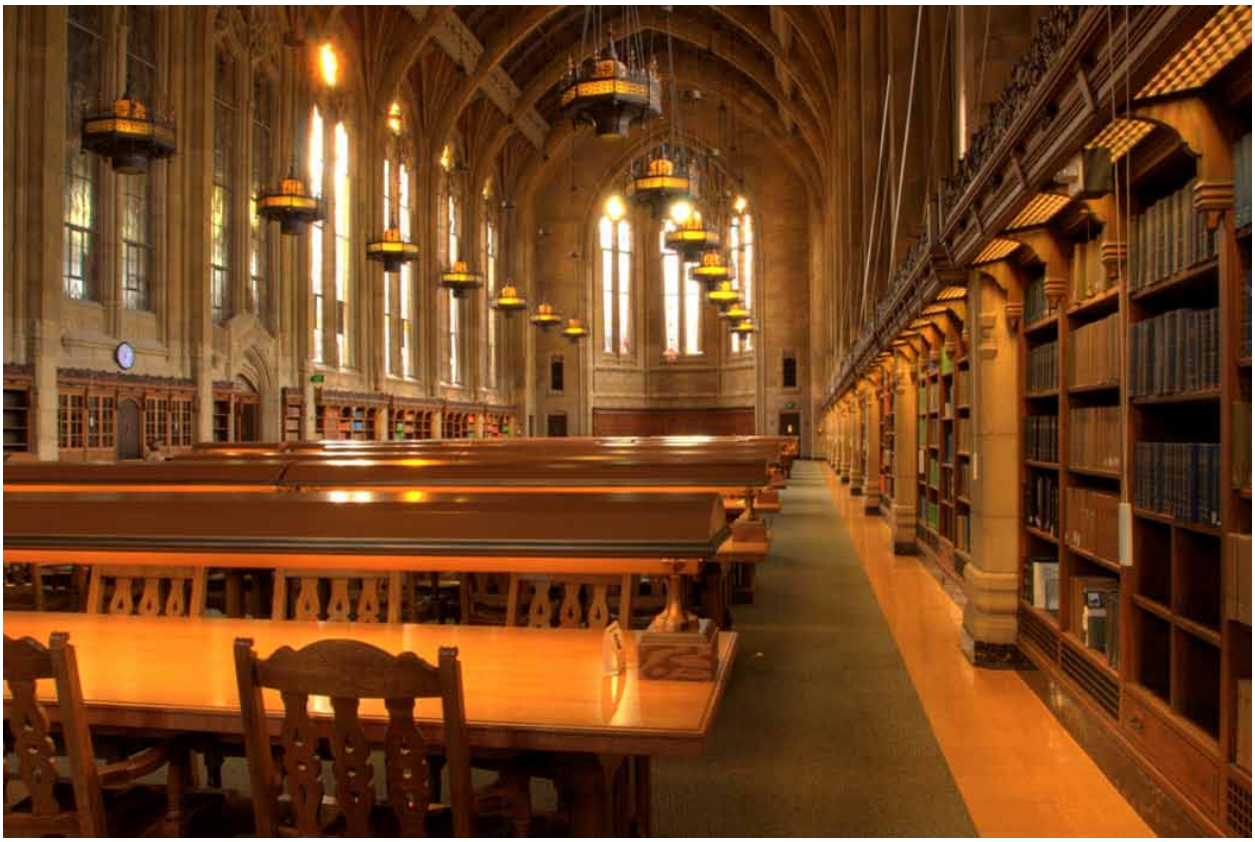
2008 Annual Report



University of Washington

ENTERPRISE RISK MANAGEMENT

University of Washington Memorandum

Date: November 2008

To: President Mark Emmert

From: President's Advisory Committee on Enterprise Risk Management

Re: UW Enterprise Risk Management 2008 Annual Report

We are pleased to provide you with a report on the University's enterprise risk management accomplishments for 2007-08. An Executive Summary is provided, which highlights the phases of development our program has gone through, noting how these parallel what has happened nationally with enterprise risk management programs. Senior leadership, campus compliance officers, and teams from key departments have continued to engage in identifying top risks and determining what actions to take to improve our risk profile, be it compliance, financial, operational, or strategic.

Follow up with risk assessments completed in 2007 demonstrates how risk owners have taken responsibility to pursue possible risk mitigation plans in their respective areas, enabling us to create a scorecard to track further progress on all assessments as they are completed.

2009 plans call for broadening our base, by refocusing the Compliance Council on financial and operational risks in addition to it regulatory ones. The President's Advisory Committee has begun discussions of key strategic risks for the institution, and this will continue as we think about the mega-risks that can impact the University's long term success.

Thank you for your continuing interest and support for this work.

In Recognition and Appreciation

Two of our colleagues who recently retired after many years of service to the University of Washington provided exceptional leadership in establishing our Enterprise Risk Management program.

Maureen Rhea – Executive Director of Internal Audit

Maureen was instrumental in formation of ERM and especially the Compliance Council. She led the Council as facilitator its first two years, establishing a forum where compliance experts from throughout the University could discuss issues of importance and share ways to improve institutional preparation and response to external requirements.

Karen VanDusen – Director of Environmental Health and Safety

Karen and her team see “risk management” as a core function in all the services they provide to campus clients. Karen set a record for participation on risk assessment teams, including serving as team leader on numerous occasions. She demonstrated how risk assessment could be used to help her management team identify its strategic priorities for the biennium, and has advocated the ERM approach and process both on campus and off.

Many thanks to both Maureen and Karen for their outstanding work on behalf of the UW and Enterprise Risk Management.

Table of Contents

I. Introduction 4

II. In Their Own Words 6

III. 2009 Recommended Goals and Directions 8
Mega-Risks Chart 9

IV. 2008 Accomplishments 11
Validation Rating Scale 15
Illustration 1: Safe Campus Progress Report 16
Illustration 2: Occupational Health and Safety Risk Summary Picture 18
Illustration 3: Privacy Oversight Group Risk Summary Picture 19
Illustration 4: Cash Handling Risk Summary Picture 20
Illustration 5: UW Animal Research Facilities Risk Summary Picture 21
Illustration 6: Impacts SE Campus Construction Risk Summary Picture 22
Illustration 7: Google Cloud Applications Risk Summary Picture 23

V. Progress Report on 2007 Assessments 24

VI. UW Compliance Council Annual Report 26

VII. CISO Risk Assessment and Scoreboard 28

VIII. ERM Self-Assessment Toolkit 32

I. Introduction

With this second annual report on UW's enterprise risk management (ERM) program and accomplishments, it is a good time to reflect on the development of our program and compare it to the evolution of the industry.

The Compliance Phase A decade ago, the concept of managing risk in a formal, consistent, enterprise-wide manner was not widely applied in the business sector, and in higher education, it was scarcely discussed. The stunning 2001 collapse of Enron and the speedy passage of the Sarbanes-Oxley Act a year later was the impetus for the first phase of ERM. Boards of directors viewed ERM as a good way to organize an entity's compliance program and to identify the most significant weaknesses in financial controls. Here at UW in 2001, we were having some experiences of our own with compliance failures, some of which were quite costly, while others negatively impacted our reputation among our students, alumni and other stakeholders.

The Governance Phase By 2004, the attorneys general of several states were conducting investigations and filing lawsuits alleging excessive CEO pay, business conflicts of interest and consumer fraud. Various consultants and associations published models for risk assessment and treatment, some emphasizing top-down leadership and others promoting grassroots approaches. During this time, ERM emerged from being primarily a compliance-focused tool and became a systematic way to inform boards of directors about the financial, operational and strategic risks which could prevent an organization from achieving its objectives.

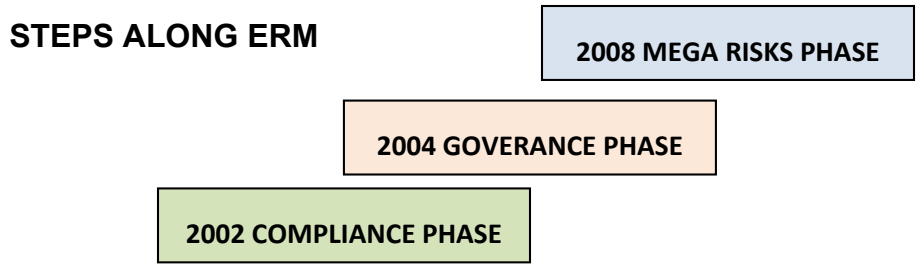
Around this time, several UW offices began to review the ERM literature and surveyed applications of the practice in higher education. In April of 2005, our new President, Mark Emmert formally charged V'Ella Warren, then-Vice President for Financial Management, and David Hodge, then-Dean of the College of Arts and Sciences, to identify best practices for managing regulatory affairs at the institutional level by using efficient and effective management techniques. We began a series of campus discussions with academic and administrative leaders about the management of risk across UW and recognized that a new layer of enforcement bureaucracy would not be accepted by the campuses; our model had to support the decentralized, entrepreneurial nature of our organization. A root cause analysis also informed us that our tendency to operate in information silos was at the heart of many of our compliance problems, and that the senior leadership did not receive truly comprehensive risk information.

Further research into ERM models led to a decision to adopt a holistic approach which would integrate broad evaluation of risk and opportunity into enterprise-wide decision-making. Although not groundbreaking theoretically, we developed a practical and interactive model in which the results of methodical risk assessments would be discussed by a Compliance Council and a President's Advisory Committee on Enterprise Risk Management. The President chartered this model in the fall of 2006 and the processes began.

In the first years, a majority of the risk assessments and discussions were dedicated to reducing the institution's liability and raising the community's awareness of risk. Several important mitigation initiatives were funded as a result of this work. As the tools were refined, we realized the value of using them to assess various business opportunities.

The Mega-Risk Phase In 2008, ERM is again evolving, with an expanded focus on the mega-risks outside the control of any entity. The impacts of recession, the uncertainties of the global marketplace, energy shocks, demographic changes, technology vulnerabilities and many other uncontrollable elements are now among the variables an entity must consider in devising its risk strategy. Rapid assessment of the risks impacting various business models is a critical element of ERM in large companies today.

UW has also begun using ERM tools in new ways: to evaluate alternative methods of financing our mission-critical operations, such as patient care facilities; to streamline and organize our units' daily operations to strategically reduce risk; and to identify emerging mega-risks that will affect us in direct proportion to our preparedness to meet them. Agility is becoming the most valuable aspect of UW's ERM program as it continues to evolve.



This year's reports highlights key accomplishments as ERM has grown throughout the University. A self-assessment toolkit is being shared with interested departments, to walk them through identifying top risks in their own operations and programs. UW's Chief Information Security Officer has taken risk assessments further, adapting the techniques to produce quarterly performance measures of security activities. Follow up on prior years' assessments has improved reporting metrics and enhanced documentation of controls for identified risks.

Recommendations for 2009 include raising the perspective to think about how mega-risks, such as extended financial crisis, may impact UW's ability to achieve its strategic goals. Improving resiliency in the University's operations is an exciting new challenge for the ERM processes. We will be using the ERM structure to address one of the institutional recommendations concerning the UW Technology business model. And our ERM program will be used in underwriting discussions with the financial rating agencies to help us maintain our credit rating. ERM continues to grow and be involved with new aspects of the University.

II. In Their Own Words

With two years of experience with our enterprise risk management program, we asked members of the President's Advisory Committee and others to share their thoughts on what ERM means to them.

"I think that the ERM process has been of great assistance in using a common metric and process to identify and address risks across a wide spectrum of the campus. Without this process/metric, it would be easier to overlook specific risks or to just attempt to deal with the risk that is in the forefront without a careful analysis of the whole picture. Also, it is easier to compare risks across a wide variety of units. In all, I think this continues to be an important and fruitful process."

Cathryn Booth-LaForce, Professor, Family and Child Nursing, and Chair of Faculty Council on Research

"As an ex officio member of the Compliance Council, [I started the year expressing that] 'compliance' was not necessarily a good word for faculty members; indeed, when I recently mentioned the culture of compliance to a colleague of mine, she said, 'that's terrible!' What lies behind such reactions, I think, is the high value faculty accord to personal autonomy. . . . The notion of a culture of compliance sounds like yet another extension of impersonal, corporate control, shrinking the arena of self-expression in favor of discipline and conformity.

". . . Having served on this Council now for nearly a year, I'm happy to report that you don't strike me as an especially grim group. . . . Indeed, I'm very impressed by the acumen and professionalism of the staff and administrators who are themselves coping with externally imposed—and enforced!—regulations. Over the last ten months, I've come to understand that you're not here to get in our way, but to make it possible for us faculty legally to conduct the work we came here to do. . . . It's equally important, however, for you to understand what it's like for faculty who are mostly just trying to make things happen so their work can go forward. . . .

"To faculty, it can appear that somebody somewhere has made a rule that's making our lives crazy, no explanation is forthcoming, and nobody cares. I know that's not how we want it to be, and that compliance officers and staff are themselves struggling with difficult issues not of their making. . . . To put it positively: the main

point of these valedictory comments is that I've come to understand your situation, and I hope you understand ours. I hope that working together, we can try to spread such understanding further, so that we can make compliance—or whatever term you choose—less threatening to faculty and frustrating to staff."

David Lovell, Research Associate Professor, Psychosocial and Community Health, and 2007-08 Vice Chair, Faculty Senate

"I think the ERM project has been very valuable. ERM is not a hard science, but it does bring a rational new discipline to identifying, weighing, and choosing among the categories of risks that inevitably face the institution. Without this rigor, it is easy to lose sight of the full range of risks and the tradeoffs involved in reducing the risks. The ERM process enables managers to assay substantial risk exposures with a common set of tools and to harmonize the standards and expectations for minimizing - and sometimes tolerating -- the downside of our activities.

"I think the goal in the coming year should be to increase the volume of programs and projects to which ERM protocols are applied. More complex, inter-departmental activities can be examined centrally while more individual departments can apply ERM techniques to review of matters that are managed entirely at their internal level."

Jack Johnson, Senior Assistant Attorney General

III. 2009 Recommended Goals and Directions

ERM continues to build on an established base of processes and tools for identifying, assessing, mitigating, and monitoring significant risks. Potential areas of beneficial activity for the coming year are outlined below, referencing the **original seven recommendations** from 2006.

A. Consider what external "mega-risks" may impact UW's ability to achieve its strategic goals. As noted in the Introduction to this year's report, uncontrollable elements such as recession, energy shocks and demographic changes are variables that every entity must consider in devising its risk strategy. We propose to use a mega-risks model (on next page) to engage the PACERM in discussions of how such risks may impact the University's ability to achieve its five strategic goals. This will contribute to the original recommendation of:

   Recommendation 1. Integrate key risks into the decision-making deliberations of senior leaders and Regents.

B. New Charter for the Compliance-Operations-Finance (COFi) Council. A review of the University's ERM efforts identified a need for the Council to go beyond a focus on compliance. The review concluded that the Council should expand its scope to include financial and operational risks. In August 2008 the Compliance Council name was changed to the Compliance, Operations, and Finance (COFi) Council to reflect this new focus. Goals for 2009 include:

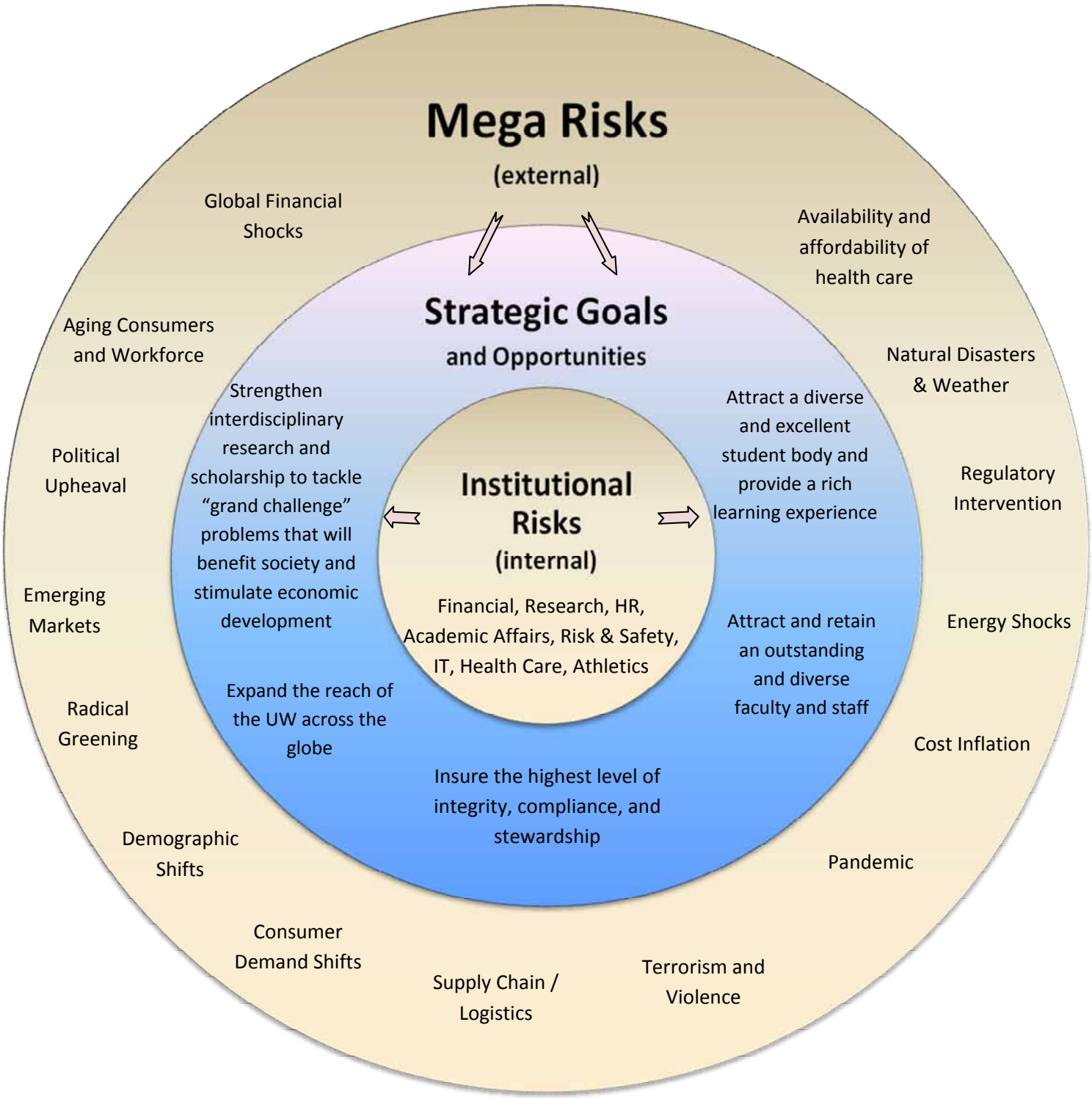
   - Implement an anonymous reporting line and compliance web-site.
   - Develop metrics for measuring and reporting achievements.
   - Provide an open forum for identifying and assessing emerging risks.
   - Continue to enhance and strengthen our culture of compliance.

   This change in focus will address three of the original recommendations:

   Recommendation 2. Create an integrated, institution-wide approach to compliance which is consistent with best practice.

   Recommendation 4. Create a safe way for interested parties to report problems.

   Recommendation 5. Minimize surprises by identifying emerging compliance and risk issues.


Mega Risks
(external)
Global Financial Shocks
Availability and affordability of health care
Aging Consumers and Workforce
Natural Disasters & Weather
Political Upheaval
Regulatory Intervention
Emerging Markets
Energy Shocks
Radical Greening
Cost Inflation
Demographic Shifts
Pandemic
Consumer Demand Shifts
Supply Chain / Logistics
Terrorism and Violence
Strategic Goals
and Opportunities
Strengthen interdisciplinary research and scholarship to tackle "grand challenge" problems that will benefit society and stimulate economic development
Attract a diverse and excellent student body and provide a rich learning experience
Attract and retain an outstanding and diverse faculty and staff
Expand the reach of the UW across the globe
Insure the highest level of integrity, compliance, and stewardship
Institutional Risks
(internal)
Financial, Research, HR, Academic Affairs, Risk & Safety, IT, Health Care, Athletics

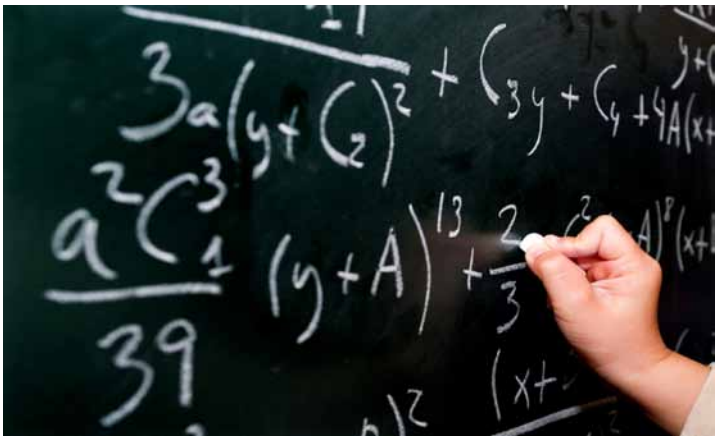
C. Continue to build the ERM program with the Office of Risk Management. ERM webpages will be enhanced. The self-assessment toolkit will be widely distributed and departments supported in their use of it. We will continue to follow up with risk owners on the progress they make with mitigation plans, and expand the monitoring to include all of the completed comprehensive assessments. Using the model developed by CISO for its own performance metrics, we will develop an institutional level version that summarizes progress on all the key risk indicators. This addresses two more of the original recommendations:

Recommendation 3. Ensure that good information is available for campus community.

Recommendation 7. Check progress on compliance and risk initiatives.

D. New audit leadership. The coming year will see the start of a new Executive Director for Audits, who will bring a new perspective on the use of enterprise risk management in identifying and assessing key institutional risks. That person will facilitate the COFi Council, and provide crucial guidance for our ERM program. This addresses another of the original recommendations:

Recommendation 6. Maintain strong audit team with ability to proactively identify problems and collaboratively recommend solutions to appropriate decision-makers.



IV. 2008 Accomplishments

The original seven recommendations from the Collaborative Risk Management Final Report (February 13, 2006) form the outline of what has been accomplished this year.

---

1. Integrate key risks into the decision-making deliberations of senior leaders and Regents.

Senior Leadership Engaged in ERM Priorities and Recommendations

The President's Advisory Committee on Enterprise Risk Management (PACERM) continued its role of identifying top risk areas for comprehensive assessments. Follow up on key risk from last year, Safety of Students, demonstrated the effort that has gone into this important topic. Open discussion of emerging risks brought forward new ideas, including a priority for the coming year to look at the risk of failing to recruit and retain top talent.

Compliance Updates for Board of Regents

UW Medicine and the Department of Intercollegiate Athletics presented annual reports on their compliance programs, and ongoing efforts to minimize risks and address current issues.

UW Medicine Patient Safety Initiatives Update

UW Medicine-Harborview Medical Center (HMC), UW Medical Center (UWMC), UW Physicians Neighborhood Clinics (UWPN) and UW Physicians (UWP) continue to focus on Patient Safety and Quality of Care as the top priority, with several major steps towards accelerating the quality agenda that include:

- Meetings with the National Leapfrog group, implementation of Leapfrog standards for quality and safety which are built on Institute of Medicine and IHI goals, and overall improvement of the publically reported Leapfrog scores for both medical centers-HMC and UWMC.
- Commissioned the University HealthSystem Consortium (UHC) to complete a focused assessment of the patient safety and quality program that included interviews with staff, physicians, management and Board members. The medical centers are utilizing the summary findings to develop the FY 09 work plan for improvement.
- Participated in the centers for Medicaid/Medicare Services (CMS) publically reported measurements (HCAHPS score) of patient satisfaction with quality of care received.
- Funded and implemented additional training modules for graduate medical education resident training to increase the quality and safety of procedures.
- Engaged in UW Medicine Board and Harborview Board level discussion to define and develop Patient Safety and Quality of Care metrics for Board review.

FY2009 Investments in Integrity/Compliance/Stewardship

Institutional investments in areas that have been included in ERM reviews include: $1.19 million for research administration support [staffing in Sponsored Programs, Human Subjects review boards, Grant and Contract Accounting, and Environmental Health and Safety compliance monitoring]; $1.8 million in administrative support [SAFE hotline, staffing in Human Resources, Internal Audit, and Information Management]; and $3 million in administrative computing systems.

New Focus on Financial Risks

Recognizing that ERM needs to expand beyond a focus on compliance, a proposal has been developed for PACERM approval to recharter the Compliance Council with an expanded scope to include financial and operational risks as well as compliance, to better respond to the full spectrum of risks and opportunities.

2. Create an integrated, institution-wide approach to compliance which is consistent with best practice.

Compliance Council continued to build networks and understanding among institutional compliance officers. Conversations included identification of UW affiliates, termed "orbiting orgs", being all the related entities who may affect University risk exposure in various ways. Differences in responsibilities between audit and a compliance office illustrated how the roles are different, yet related. See the full Compliance Council report beginning on page 26.

In 2007, the Council produced the first institutional compliance risk map. During this year, more than a third of Council members provided further information about their existing procedures, training, monitoring, and other controls which address their specific compliance risks. This information fills in the institutional Risk Register, documenting the efforts to achieve compliance.

The Office of the Chief Information Security Officer (CISO) took these efforts a step further, using risk identification and assessment as a basis for creating a program performance scorecard; this work is described beginning on page 28.

3. Ensure that good information is available for campus community.

ERM's standard processes for risk identification and assessment, using common rating scales for likelihood and impact, have been incorporated into a "self-assessment toolkit" with the intent of encouraging departments and units throughout the University to apply ERM to their own operations. The toolkit is discussed beginning on page 32, and the complete toolkit booklet is provided as an attachment to this report.

The ERM program has been assigned within the Office of Risk Management, which itself is now part of the Treasury Office. ERM webpages are available through the Risk Management website.

4. Create a safe way for interested parties to report problems.

UW SafeCampus Update

The Violence Prevention and Response Program, introduced in 2007, received permanent funding and is now staffed with a team experienced in violence prevention, victim advocacy and program management. Three SAFE phone lines operate 24 hours a day, seven days a week, serving the Seattle, Bothell and Tacoma campuses. Phone response staff helps callers clarify their concerns, identify immediate risk mitigation steps, connect callers with University or community resources, and arrange for follow-up as needed.

A SafeCampus public information campaign has been developed (for launch September 2008) to raise awareness of how violence can enter and affect our community, and of the University's policies and programs designed to prevent and respond to threats of violence. The campaign will center on publicizing violence prevention and response resources, policies, and training opportunities on the Seattle, Tacoma and Bothell campuses.

Other program developments, including the volume of services provided, are outlined in a progress report SafeCampus Progress Report/January 2008-August 2008 (see illustration #1 on page 16).

Development of UW Reporting Line

Additional work on determining how to establish an anonymous reporting line at UW included: meeting with two peer institutions to discuss how their reporting lines work; meeting with a few providers of reporting line services to understand the range of possibilities for this service; and discussions led by Internal Audit with senior leaders to identify questions they may have in how a reporting line may be implemented at UW.

5. Minimize surprises by identifying emerging compliance and risk issues.

Comprehensive risk statements were completed for the following priority topics:

- Occupational Health and Safety – Campus experts assessed general exposures, protection and training, systematic factors and costs that can impact the health and safety of faculty and staff.
- Privacy – Patient privacy officers identified and assessed key risks around the use and handling of confidential patient information.
- Cash Handling – Follow up to a state audit review, the assessment team looked at areas of potential loss for both central and campus units that handle and deposit cash.

- Animal Research Facilities Alternatives – Accreditation requirements determine the spaces suitable for conducting animal research; as pressures grow for such space, alternative investment options were considered for meeting the top risks.
- Southeast Campus Construction Impacts – The Sound Transit project is moving towards start of construction; this team brought together departments whose members and visitors/patients will be affected to identify key mitigation planning efforts.
- Cloud Computing Alternatives – Opportunities exist to use computing capacity and storage at large organizations, such as Google, to provide services for campus users at little or no cost; however, such remote and independently operated sites raise compliance concerns for privacy of student records, and ability to produce records when legally required to do so; this assessment looks at several alternatives which can be used to address those risks.

The top risk Summary Pictures for these assessments follow this report (see illustrations 2 to 7, beginning on page 18).

As noted above with the new focus on financial risks, the Compliance Council charter is proposed to add financial and operational risks. PACERM will enhance its strategic perspective, with discussions of "mega risks" that may impact UW; see 2009 Goals.

6. Maintain strong audit team with ability to proactively identify problems and collaboratively recommend solutions to appropriate decision-makers.

The Internal Audit department was expanded from 9 to 15 audit staff. Audit teams were restructured and additional auditors were hired with expertise in research compliance and information technology. A separate audit team was established and responsibility for performing audits of UW Medicine was transferred to Internal Audit.

7. Check progress on compliance and risk initiatives.

ERM followed up on progress by risk owners from the 2007 assessments, as to how they are addressing top risks. A format was developed to relate the original risk level with an updated risk level based on any mitigation in the past year. This model also identifies gaps between what the ideal risk level will be when mitigations are complete versus what the current level of risk is—a way for risk owners to think about priorities as they continue to manage their top risk areas. The progress reports are discussed further beginning on page 24.

Validation Ratings

The following factors are considered in validating the level of analysis and risk ratings (likelihood and impact) for each completed risk summary picture (for reference with the risk summary pictures on pages 18 to 22).

	Basic Level	Intermediate Level	Advanced Level
Quantitative Analysis	Minimal data Quantification of selected few risks, typically compliance or financial	Review of some UW data Quantification of multiple risks, including operational risks	Analysis of UW data such a loss claims, EHS incident reports Continuous feedback/ assessment of data
Qualitative Analysis	Reliance on people for information: opinion poll, anecdotes, case studies of UW experiences	More complete collection, review of UW experience Review past audit reports Consideration of peer/ industry best practices	Documented evidence of UW multi-year trends Significant analysis/ comparison of UW with others, such as peer or industry studies
Team Expertise	UW team with general knowledge of risk area and requirements for compliance, financial, operations, and strategic	UW team with expert knowledge and experience in risk area	UW experts and outside expertise/analysis
Other Factors	Risk transfer: - Commercial insurance, self-insurance ; or - Contract requirements	Regulatory examinations and other periodic, formal external reviews or accreditation	Actuarial analysis Financial analysis/ UW Treasury

SafeCampus www.washington.edu/safecampus

Progress Report | January 2008 – August 2008

RESOURCES

- Permanent funding established for the Violence Prevention and Response Program (VPRP).
- Recruited and trained VPRP staff with expertise in violence prevention, victim advocacy and program management.
- UW Police Department appointed new victim advocate position responsible for assisting crime victims and their families, and witnesses through the process of physical, emotional and financial recovery.
- Rape Aggression Defense (RAD) Program added to UW Police Department-sponsored programs in August 2008. Enrollment open to UW community free-of-charge.
- Health & Wellness, a unit within StudentLife, established to work directly with students who may need a higher level of support and individual attention.
- UW Outdoor Alert system successfully tested after UW Technology installed 12 new Talk-a-Phone towers, which were approved by the Emergency Management Planning Committee as part of the UW's ongoing work to improve emergency communications.

COMMUNICATIONS, OUTREACH & TRAINING

- SafeCampus website averaged 162 visits per day.
- UW Alert registered 10,276 subscribers to receive emergency notifications by email and text messaging.
- Marketing materials and redesigned website produced for SafeCampus public information campaign starting in September 2008.
- 1372 people attended in-person training sessions (46 department-specific training sessions provided by UWPD and HR Operations; 13 campus-wide training sessions open to faculty, staff, and students; 54 safety talks/worksite security reviews conducted by UWPD)
- Violence prevention and response resources promoted at nine University events, including fairs at UW Bothell and UW Tacoma.

POLICY

- Implemented new legal provisions that assist victims of domestic violence, sexual assault, or stalking.
  - **Employment Leave for Victims of Domestic Violence (SHB 2602).** Employees who are or whose family members are victims of domestic violence, sexual assault, or stalking are entitled to reasonable leave to seek legal advice; find medical treatment, mental health or social services; obtain shelter; or participate in safety planning. Effective April 1, 2008.
  - **Shared Leave Sharing for Victims (SSB 6500).** Extends shared leave eligibility to employees who are victims of domestic violence, sexual assault, or stalking. Effective October 1, 2008.
- UW Police coordinated the compliance with the **Campus Safety and Security Act (SSB 6328)** by gathering information from other departments and organizing a uniform report format with other WA institutions of higher education.

STATISTICS

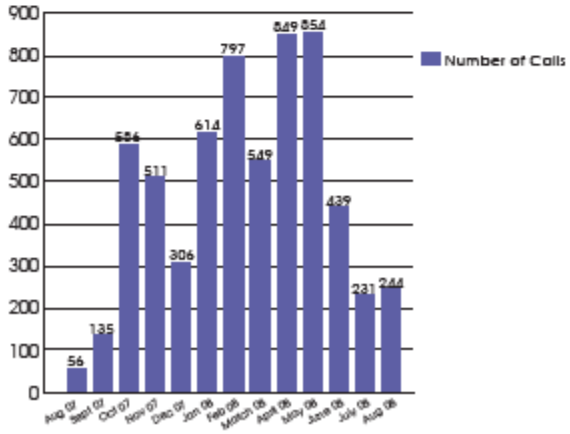
UW CareLink Utilization for individual consultations increased by 47% over the same period the previous year.

- January–June 2008: 945 individual consultations
- January–June 2007: 643 individual consultations

UWPD Crime Victim Advocacy Assisted over 35 students, faculty, and staff members. Services included:

- Enrolled three victims in the Washington State Address Confidentiality Program.
- Conducted 15 court accompaniments for victims petitioning for protective court orders.
- Assisted three victims in applying for Crime Victims Compensation.
- Facilitated the legal breaking of three apartment leases under RCW 59.18.575.

Husky NightWalk



SafeCampus www.washington.edu/safecampus

Progress Report | January 2008 – August 2008

Violence Prevention & Response Program

- Calls to SAFE phone number reported 246 issues of concern and 45 requests for information/materials from January 2008 – August 2008.
- 58 assessments from January 2008–August 2008.

Note: Previous Progress Reports included the number of assessments and "case reviews." In January of 2008, VPRP in cooperation with campus partners re-evaluated how calls were triaged and eliminated the category "case reviews." The new classification system follows:

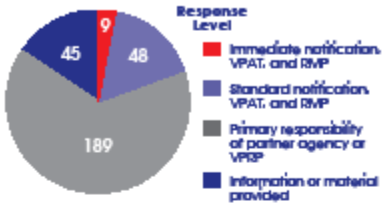
Level 1: Violence Prevention Assessment Team (VPAT) is notified and convened as soon as possible.

Level 2: Issue is discussed at next scheduled VPAT meeting (VPAT meetings are held three times per week).

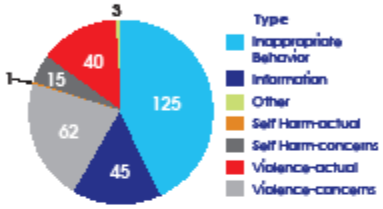
Level 3: These situations require the same level of communication with the caller and analysis as other Response Levels. Situations assigned Response Level 3 do not have a VPAT. Instead, VPRP is responsible for monitoring and following up on required risk mitigation strategies or they are referred to other UW departments to be the lead and carry out further actions required—while keeping VPRP informed of developments.

Level 4: Request for information/materials or not UW jurisdiction.

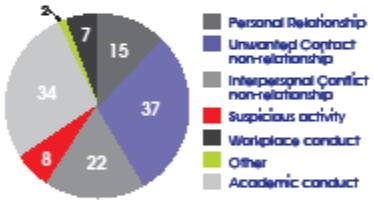
Number of Issues Reported - 291 total



Count by Issue Type - 291 total



Inappropriate Behavior Detail - 125 total



	Role of the Person Experiencing the Concern	Role of the Person Causing the Concern	Role of the Person Reporting the Issue
UW Faculty - Non Supervisor	23	11	11
UW Faculty - Supervisor	4	3	13
UW Graduate Student	1	1	0
UW Graduate Student Employee	6	3	1
UW Staff - Non Supervisor	88	42	57
UW Staff - Supervisor	23	6	83
UW Undergraduate Student	42	23	12
UW Undergraduate Student Employee	20	11	6
VPRP Partner	0	0	74
Public	4	6	2
Public (Patient)	2	24	0
Public (Personal Relationship)	3	35	8
Public (Previous UW Affiliation)	3	10	0
Unknown Identity	0	14	0
Other	2	1	2

Illustration 2

Occupational Health and Safety – Risk Summary Picture

Risk Assessment Work Group:

Stan Addison, Paul Brown, Thea Brabb, Robert Carroll, David Emery, Ron Fouty, Carol Garing, Norma Jean Haulman, David Kalman, JoAnn Kauffman, Dave Leonard, Bruce Miller, Erin Ondrak, Gary Pederson, Lou Pisano, Patricia Riley, Ellen Rubin, Denis Sapiro, Shari Spung, Stephanie Steppe, Michael Welch, Melinda Young, Karen VanDusen, Karen Zaugg, David Zuckerman

TOP RISKS	Current Environment
Employee protection & training: Inadequate personal protection, training, monitoring and emergency preparation for researchers, staff and faculty cause short and or long term safety/health hazards, injury, illness or death	
General exposures: Environmental releases/excess exposure to physical, chemical, biologic, ionizing and non-ionizing radioactive, and/or other workplace hazards result in faculty, staff, or student injury, illness or death	
Systemic factors and strategic planning: UW research practices, risks, and/or lab acquired illnesses result in negative media coverage and negative impact on UW image/fund raising/reputation	
Systemic factors and strategic planning: Insufficient resources to provide comprehensive oversight of workplace and research risks/practices hinders research enterprise and ability to anticipate risks to employees, students, resulting in injury or illness	
General exposures: Employees/students injured as a result of acts of violence	
Research factors: Use of infectious agents or other hazardous materials without approval, adequate controls or monitoring causes disease/illness	
Long term costs: Insufficient NIH safety compliance regarding biosafety and animals leads to funding loss and capital costs	
Systemic factors and strategic planning: Insufficient process to deliberately and systematically identify health and safety risks leads to inadequate prevention and control of risks	
General exposures: Work being done by contractors & other non-UW employees' causes Injuries, illnesses, exposures to UW employees/students	
Decentralization of academic programs: Decentralization, turnover, inexperience hinders control programs for injury prevention, particularly in Academic side	
Long term costs: Increased costs and hazards due to limited consideration of environmental health and safety construction issues (e.g., codes, standards, accreditations) in renovation or new construction of labs or other facilities	

Validation Rating: **INTERMEDIATE.** UW team with expert knowledge and multidisciplinary experience in occupational health & safety, compliance requirements and internal controls. Assessment includes knowledge of University incidents/accidents, workers' compensation experience factors, fines and other regulatory reviews.

Patient Privacy Oversight Group – Risk Summary Picture

Illustration 3

Risk Assessment Work Group:

Tara Adolfi, Jane Fellner, David Hays, Stephanie Jellison, Colleen Johnson, Eunice Little, Suzanne McCoy, Richard Meeks, Christopher Norton, Shelly Oosterman, Marcia Rhodes, Ellen Rubin, Bekki Sanchez, Tina Sheldon, Johanna Taylor, Addie Price, Catherine Thieman

TOP RISKS	Risk Evaluation based on:		
	Without Controls	With Controls	With New Controls "Mitigation"
Verifying the Identity & Authority of Individuals Requesting Access or Disclosure: Inappropriate use/access of PHI			
Verifying the Identity & Authority of Individuals Requesting Access or Disclosure: Workforce members releasing specially protected PHI			
Training: Workforce members, including volunteers, management & students, not completing required training			
Verifying the Identity & Authority of Individuals Requesting Access or Disclosure: Workforce members releasing PHI outside their scope of work			
Decentralized structure: UW Medicine's decentralized structure results in inconsistent investigations, inconsistent sanctions, inconsistent hiring, rehiring practices, and fragmented Medical Record documentation.			
Verifying the Identity & Authority of Individuals Requesting Access or Disclosure: Workforce members releasing PHI not for Treatment, Payment, Healthcare Operations; under an authorization by a patient; or when mandated/permitted by law			
Research: Accessing PHI for research without IRB approval			
Access: Not deactivating access to PHI in a timely manner			
Access: Provide PHI access outside workforce member's job duties			
Fundraising & Marketing: Patients misperception that UW Medicine is using PHI for fundraising			
Memorandums of Understanding: Providing access to non-UW individuals then these individuals using and/or disclosing PHI inappropriately			
Accounting Disclosures: Disclosing PHI that is mandated by law without accounting for disclosure			
Training: Privacy, Confidentiality, and Information Security Agreement are not being signed by workforce members at job performance evaluations / re-credentialing			
Access: Inappropriate collection and use of social security numbers			

Rating Validation: **INTERMEDIATE**. Excellent team expertise in all aspects of privacy, compliance requirements, current UW operations and internal controls. Known frequency of privacy events, fines; experience with investigations and external regulators.

Illustration 4

Cash Handling – Risk Summary Picture

Risk Assessment Work Group:

William Christensen, Tess Domingo-Herrera, Jeff Follman, Evelyn Jagoring, Karen Long, Sandie Rosko, Gina Salois

TOP RISKS	Risk Evaluation based on:		
	Without Controls	With Controls	With New Controls "Mitigation"
State of Washington Admin. & Accounting Manual: UW departments are not in compliance with cash handing policies			
Revolving Funds: Funds are Misappropriated			
Field Advances: Funds are Misappropriated			
Field Advances: Financial Records are Incorrect			
Small Decentralized Units That Direct Deposit: Funds are Misappropriated			
Large Decentralized Units that Direct Deposit: Financial Records are Incorrect			
Central Units: Funds are Misappropriated			
Large Decentralized Units that Direct Deposit: Funds are Misappropriated			
Revolving Funds: Financial Records are Incorrect			
Central Units: Financial Records are Incorrect			
Departments who receive small amounts of cash and transmit to SFS: Funds are Misappropriated			
Small Decentralized Units That Direct Deposit: Financial Records are Incorrect			
Departments who receive small amounts of cash and transmit to SFS: Financial Records are Incorrect			

Rating Validation: **INTERMEDIATE**. Excellent team expertise in all aspects of cash handling requirements, current UW operations and internal controls. Analysis of transaction volume and audit results.

Animal Research Facilities Plan – Risk Summary Picture

Risk Assessment Work Group:

Kathryn Waddell, Dave Anderson, John Chapman, Michael Carette, Denny Liggitt, Nona Phillips, Colleen Pike, Chris Malins, Jill Morelli, Stephanie Steppe, Oliva Yang, Jim Angelosante

TOP RISKS	Risk Evaluation based on three options:		
	No Further Investment	Remodel & Improve	Build New & Expand
Unable to maintain AAALAC accreditation, USDA Registration and UW's Animal Assurance			
Increasing requirements for specialized research space			
Unable to recruit & retain key research faculty, staff, and graduate students			
Not competitive for new grants and contracts			
Unable to sustain and expand animal census. Reduction in animal census and procedural areas due to space constraints			
Reputation risk for competitive research edge			
Physical harm to researchers, staff and animals			
Unable to maintain adequate support for teaching and research mission			
Investment costs increase due to construction inflation and/or interest rates increase, increasing the cost of borrowing			
Require additional University financial support			
Competing construction projects for South Campus space			

Rating Validation: **BASIC**. A first effort to identify risks associated with funding future Animal Research Facilities. Analysis of three options based on a team of campus experts with extensive knowledge and experience in risk areas.

Illustration 6

SE Campus Impacts from Construction Projects – Risk Summary Picture

Risk Assessment Work Group:

Jim Angelosante, Natalie Bankson, Alex Berezow, Andy Casillas, Jeff Compher, Peter Dewey, Theresa Doherty, Chip Lydum, Ralph Robinson, Daniel Schwartz, Helen Shawcroft, Stephanie Steppe, Chuck Treser

TOP RISKS	CURRENT Environment-Controls-Plans
Interrelated Projects: Project delays and cost increases for other UW construction, due to competition for trucks, labor, and roadways from Sound Transit project, and others.	
Street Traffic: Emergency vehicles, public transportation, shuttles, other UW operations disrupted due to traffic congestion.	
Revenues: Decline in revenues for UWMC Dentistry Athletics Waterfront Activities Ctr visits, rentals, reserv	
Parking: UW, UWMC, Dentistry, ICA visitors, faculty, staff, students and/or patients encounter greater challenges in finding parking.	
Health and safety: Increases in jaywalking, pedestrian/bicyclist injuries and near misses.	
Health and Safety: Concern for appropriate, nearby evacuation and assembly surface space (game days, large events, disaster planning and preparedness).	
Financial impacts: Increased UW operating costs (e.g. devote existing staff or hire new staff to coordinate for project impacts)	

Validation Rating: **INTERMEDIATE**. Good representation of units and programs to be impacted during construction. Excellent team expertise in all aspects of current UW operations, and majority of assessment team members knowledgeable about UW transit plans and impacts through participation in prior committees and meetings. Significant financial impact analysis by major units (UWMC, Athletics, Parking). Participation by UW Project Manager to provide information about plans and agreement terms.

Illustration 7

Google "Cloud Application" – Risk Summary Picture

Risk Assessment Work Group:

TOP RISKS	Option #1 – Current business operating environment	Option #2 – Current business operating environment with additional funding for strategic security initiatives	Option #3 – Risk associated by adding authorized cloud computing (incl Option 2) with standard contract and SAS 70 controls	Option #4 – Risk associated by adding authorized cloud computing (incl Option 3) and negotiated contract with additional security controls
Large data caches with confidential data (databases and large data files) >100k individuals or >$250k loss [note these risks are similar for individual data caches/smaller databases and loss; impact somewhat lower for unnecessary breach notification/costs]				
Unnecessary breach notification, associated costs and reputational loss				
Data collection by nation states				
Theft of data by organized crime				
Risk ratings improve compared to current environment under options 3 and 4 for following: - Failure to meet data control requirements of state/federal regulations and contract obligations - Sanctions by regulators for compliance failures - Liability of civil action for loss of data - Loss of data integrity - Loss of access to data				
Federal Rules of Civil Procedure (FRCP) – includes email and documents: Risk ratings improve compared to current environment under options 2, 3 and 4 for all identified risks: - Failure to respond to court request in a timely manner - Failure to be able to freeze records - Failure to provide all related data - Failure to demonstrate reasonable operational practices (due care)				
Data classified as public and restricted (email and information sharing tools): Risk ratings improve compared to current environment under options 2, 3 and 4 for all identified risks: - Failure to meet data management compliance requirements (WA data retention rules, IRS related data) - Failure to provide enforcement for codes of conduct (appropriate use) - Failure to protect intellectual property interests - Data collection by nation states, or theft of data by organized crime				

v. Progress Report on 2007 Assessments

One of the accomplishments during the first year of enterprise risk management was to produce the University's first Institutional Risk Map, illustrating the top compliance, operations, financial and strategic risks. These risks were identified through comprehensive assessments of risk topics identified by PACERM as priorities for 2007.

As part of each assessment, the evaluation teams identified potential mitigations which they believed would reduce the institution's exposure in specific risk areas. During this second year of ERM work, each risk owner was asked to provide an update on mitigations that have been taken or put in place. Based on their assessment of those mitigations, and on any changes in their environment and in their programs or operations, the risk owners were asked for their judgment on the current likelihood and impact of each of the 2007 key risk statements.

The comparison of changes in risk exposure on these key risks is illustrated below.

Compliance Risks	2007	2008
Post-Award Financial Admin		
Post-Award Financial Admin		
Global Support		
Post-Award Financial Admin		
Asbestos		
Asbestos		
Student Safety		
Pollution		
Student Safety		
Pollution		

Operations Risks	2007	2008
Student Safety		
IT Security		
IT Security		
IT Security		
Global Support		
Student Safety		
Asbestos		
Global Support		
Global Support		
Pollution		
Pollution		

Financial Risks	2007	2008
Post-Award Financial Admin		
Post-Award Financial Admin		
IT Security		
Global Support		
Pollution		

Strategic Risks	2007	2008
Student Safety		
IT Security		
IT Security		
Pollution		
Global Support		

A number of risk areas, notably Student Safety and Post-Award Financial Administration, were able to somewhat reduce the highest risks through efforts in the

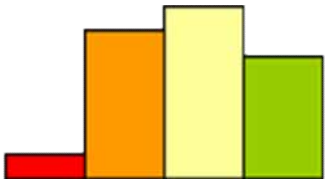
past year. Another view of how overall institutional risks in these categories has been reduced is shown below.

2007

Highest Likelihood
Highest Impact

Lowest Likelihood
Lowest Impact

Extreme	6%
High	32%
Substantial	35%
Medium	26%
Low	- -



2008

Highest Likelihood
Highest Impact

Lowest Likelihood
Lowest Impact

Extreme	- -
High	45%
Substantial	23%
Medium	32%
Low	- -

The ERM program will continue to assist risk owners who perform annual mitigation reviews and assessment updates. A goal for the coming year is to develop an institutional risk scoreboard along the lines of the one that is discussed in the section of this report on CISO Risk Assessment and Scoreboard.

VI. UW Compliance Council 2008 Annual Report

Since 2006 the University of Washington has engaged in an Enterprise Risk Management program. As part of that program, the Compliance Council represents the University's strategy for creating a more comprehensive institutional risk perspective without sacrificing existing organizational structures. It is the formal mechanism for convening representatives from each significant institutional compliance area.

The Council is organized under the umbrella of the President's Advisory Committee on Enterprise Risk Management (PACERM). The Council includes 25 members representing 19 different compliance areas within the University. Meetings are facilitated by the Executive Director of Internal Audit, and were held seven times over the past year.

A Steering Committee is responsible for directing the work of the Council, making recommendations to PACERM on the Council's work plan, and acting as the subject matter expert/liaison for risk assessments or projects. The Committee members include representatives from the key UW-wide compliance areas of research, patient care, human resources, business services, IT security, risk management, and internal audit.

2008 Compliance Council Goals and Accomplishments

During the past year the work of the Council was focused around four key goals.

1. **Enhance and strengthen our culture of compliance.**

   The Council was introduced to the culture of compliance pyramid. The pyramid identifies the key elements that make up a model compliance program and helps provide an understanding and awareness of how to achieve our goal of an on-going "culture of compliance".

   There are a variety of organizations that are closely affiliated with the University, or which the University is a member of such as the UW Alumni Association, Husky Fever, or Seattle Cancer Care Alliance. The Council explored the relationship of these organizations to the University and obtained an understanding of the types of risk that they represent to the University.

   In an effort to enhance Council members' knowledge of compliance, Council meetings included presentations on the UW research enterprise, a comparison of academic healthcare compliance programs to the internal audit function, business continuity and essential services, the state ethics law, and use of the Enterprise Risk Management toolkit for risk identification and assessment.

2. **Provide employees with a safe place to raise compliance and ethics concerns by implementing an anonymous reporting line.**

The purpose and reason for implementing an anonymous compliance and ethics reporting line at the University was discussed with the Council. This information was shared with key faculty, administrators, and staff throughout the University to obtain their input and any concerns that may need to be addressed.

In February, a special meeting was held to provide Council members with the opportunity to learn about the compliance and ethics reporting lines at Michigan and Ohio State Universities. Presentations were made by the Directors of Internal Audit on how their reporting lines were structured, the implementation process, and lessons learned.

Work has begun on drafting the guiding principles and standard operating procedures for the anonymous reporting line. This project will continue on into 2009.

3. **Support compliance training and outreach by launching a compliance website.**

   In 2007 the Steering Committee agreed on a format for the website. During 2008 a University wide survey was completed to identify what areas/departments are currently handling what types of compliance issues or complaints. This information will provide the basis for developing a useful and informative web-site.

4. **Focus on providing an open forum for identifying and assessing emerging risks.**

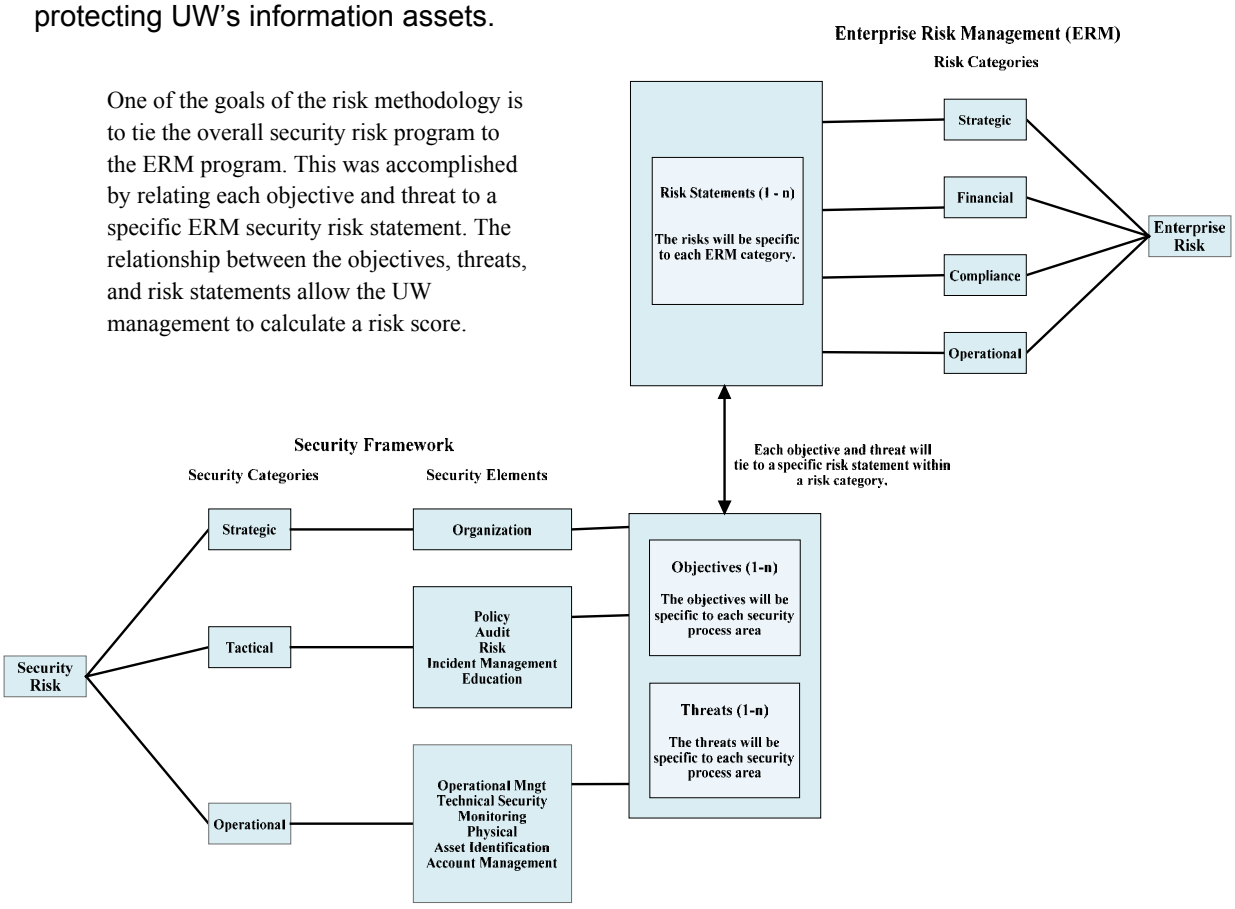
   Council meetings provided a supportive forum for discussing and vetting emerging compliance issues. Members discussed evolving issues in the areas of sponsored research, health and safety, human resource management, IT security, public information requests, and changes to the state whistleblower regulations.

   The Steering Committee's planning for 2009 Council activities led to development of a recommendation to expand the Council beyond a focus on compliance, by adding operational and financial risk considerations to the Council's work. A revised Council charter has been developed and will be submitted to the PACERM for its endorsement.

vii. UW's Office of the Chief Information Security Officer Takes Risk Identification and Assessment to New Levels

UW's Office of the Chief Information Security Officer (CISO) has embraced ERM and risk assessments as a valuable process for identifying and gauging the degree of threats for information technology. The Office of the CISO participated in the Compliance Council's compliance risk map and led a comprehensive assessment of information security risks. The top risks from the assessment helped establish the priorities to direct additional resources for protecting UW's information assets.

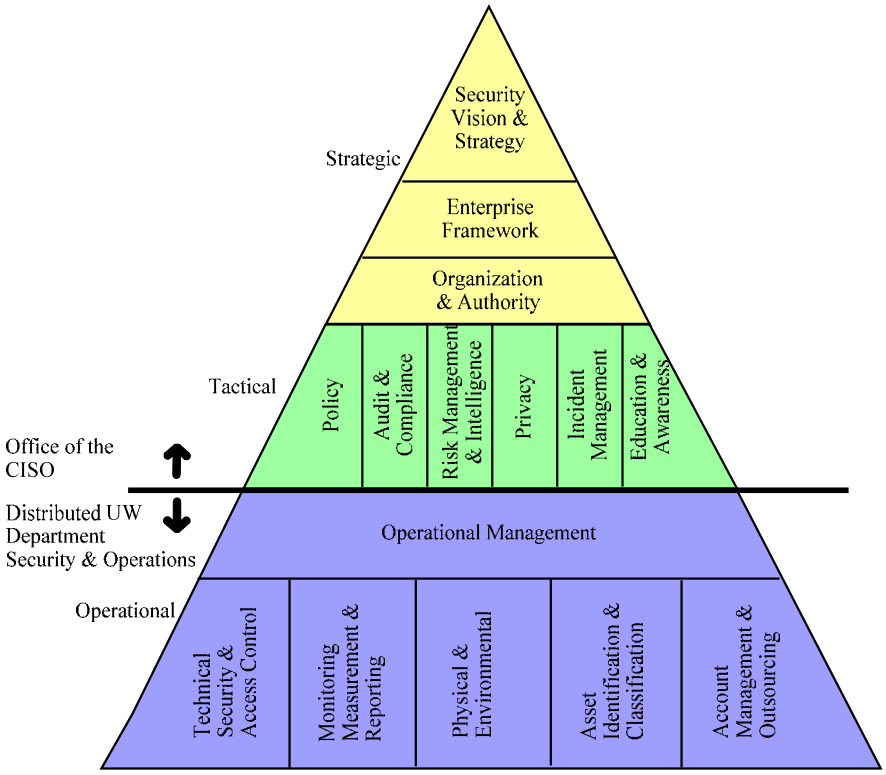
One of the goals of the risk methodology is to tie the overall security risk program to the ERM program. This was accomplished by relating each objective and threat to a specific ERM security risk statement. The relationship between the objectives, threats, and risk statements allow the UW management to calculate a risk score.



The Office of the CISO has taken the ERM process further: *"A fundamental accomplishment was the development and adoption of the Office of the CISO risk management tools and scorecard. The tools provide a valuable focus on our performance and resource expense. More importantly, publishing our scorecard provides a widely acceptable medium for UW management to understand how the Office of the CISO is addressing information security challenges. The strategic plan and security elements are based on risk tools and provide an effective compass." (September 2008 Office of the CISO Quarterly Risk and Scorecard Report)*

This model of developing a comprehensive scorecard for all the applicable risks will be used as a basis for developing standard reporting in all of UW's major risk areas. We commend CISO for this excellent work.

The scorecard is based on Strategic Security Elements, responsibility for which is split between the Office of the CISO and UW departments.



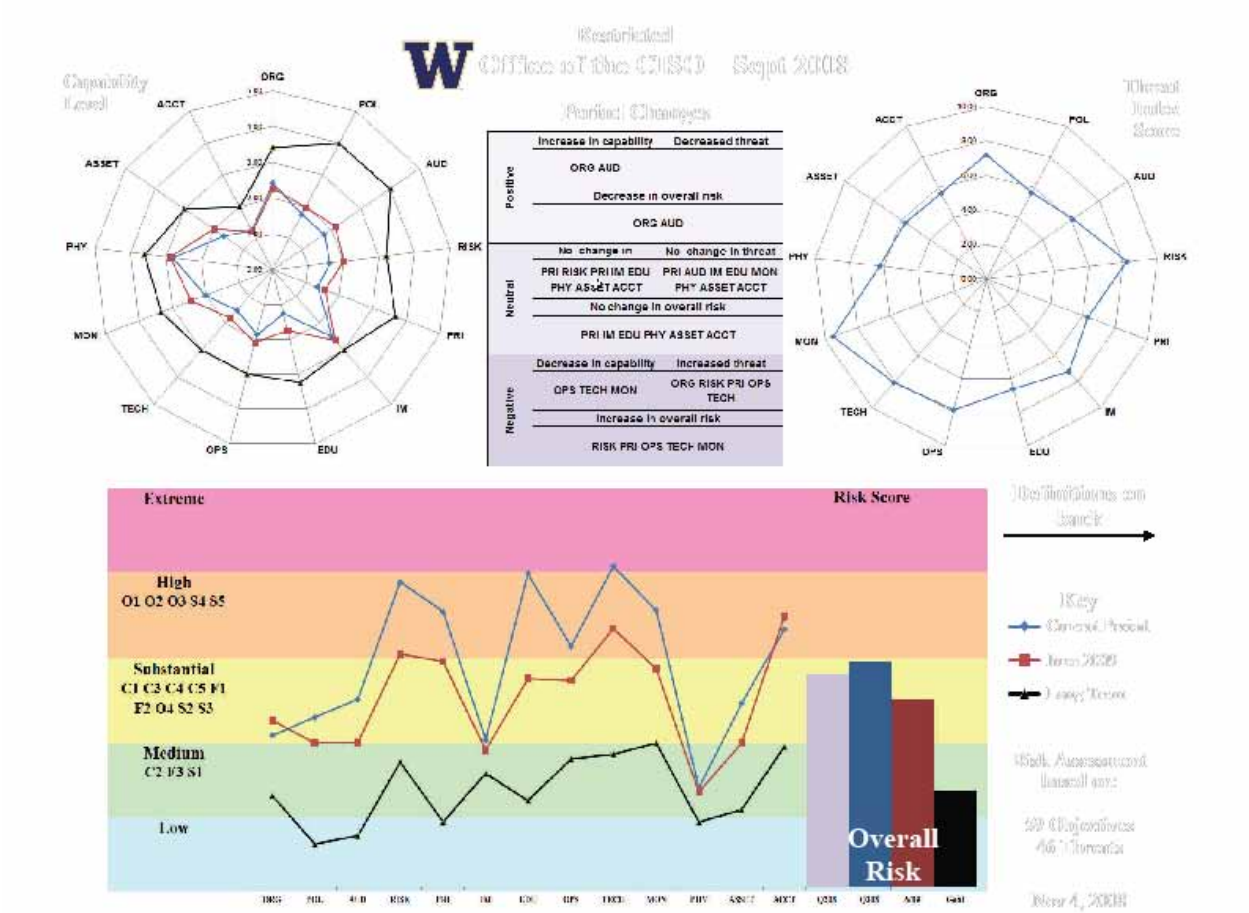
Each Strategic Security Element is evaluated quarterly for:

Capability Level: level of capability the organization has reached in developing its comprehensive security program for each security element. Capability level is five point scale.

Threat Index Score: Based on likelihood, impact and confidentiality-integrity-availability (CIA) relationship. Impact determined by damage caused to the asset or organization by vulnerability exploitation calculated by adding the likelihood score, impact score, and one point for each CIA relationship to the threat.

Risk Score: Represents overall risk in each element, calculated by formula: *Threat Index Score ÷ Capability Level*

Both Capability Level and Threat Index Score are plotted on the following "radar" diagrams, and Capability is assessed at the current level, what is expected to achieve this fiscal year with available resources, and the long term goal. The Risk Score for each Security Element is plotted on the following graph along with the ERM Risk Categories. The graph also shows the overall risk for the last and current reporting period, end of fiscal year, and long term goal.


ORG
POL
AUD
RISK
PRI
IM
EDU
OPS
TECH
MON
PHY
ASSET
ACCT
Positive
Increase in capability
Decreased threat
ORG AUD
Decrease in overall risk
ORG AUD
Neutral
No change in
No change in threat
PRI RISK PRI IM EDU PHY ASSET ACCT
PRI AUD IM EDU MON PHY ASSET ACCT
No change in overall risk
PRI IM EDU PHY ASSET ACCT
Negative
Decrease in capability
Increased threat
OPS TECH MON
ORG RISK PRI OPS TECH
Increase in overall risk
RISK PRI OPS TECH MON
Extreme
Risk Score
High
O1 O2 O3 S4 S5
Substantial
C1 C3 C4 C5 F1
F2 O4 S2 S3
Medium
C2 I3 S1
Low
Overall
Risk

Security Framework Categories

ORG	Organization & Authority
POL	Policy
AUD	Audit & Compliance
RISK	Risk Management & Intelligence
PRI	Privacy
IM	Incident Management
EDU	Education & Awareness
OPS	Operational Management
TECH	Technical Security & Access Control
MON	Monitoring, Measurement, & Reporting
PHY	Physical & Environmental Security
ASSET	Asset Identification & Classification
ACCT	Account Management & Outsourcing

ERM Risk Statements

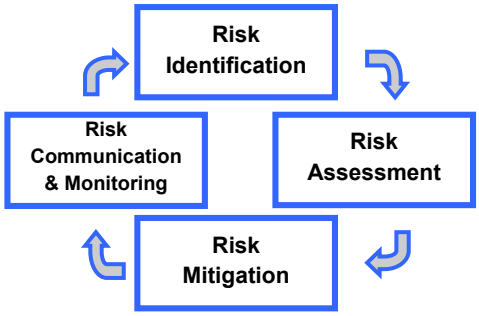
C1	Failure to meet diverse, contradictory, or unmanageable compliance requirements
C2	Sanctions and limits on business
C3	Reputation loss or competitive disadvantage due to failures related to voluntary or obligatory compliance
C4	Loss of merchant accounts
C5	Criminal liabilities
F1	Regulatory sanctions, fines, judgments, and settlements
F2	UW failures created financial loss
F3	Vendor or business partner failures create financial loss
O1	Loss, disruption or unauthorized use of computing resources
O2	Loss, degradation or unauthorized access of network/ telecommunication resources
O3	Destruction, corruption, loss, or theft of information
O4	Theft, destruction, or unauthorized access to facilities or assets
S1	Unnecessary financial costs
S2	Unable to correct high risk incidents or behavior upon notice
S3	Loss of competitive advantage
S4	Missed legal and regulatory interests
S5	Missed business opportunities

VII. ERM Self-Assessment Toolkit

The first year of UW's enterprise risk management (ERM) program developed and refined a number of processes and tools used in conducting comprehensive risk assessments. As we gained experience with more and diverse evaluation teams, it became clear that with some guidance, the ERM process could be used by individuals and departments to conduct their own risk assessments.

Andrew Faris, ERM Analyst, pulled together these materials and created a four-step self-assessment manual based on a standard risk management process.

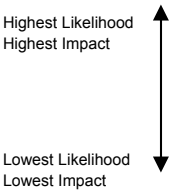
Risk Management Process



The toolkit starts by asking users to think about the ERM development model, and understand the levels of outcomes, activities, risk and control optimization that are possible. Users are encouraged to begin with a "Basic" assessment that will increase risk awareness and education among those who participate. Examples from prior comprehensive assessments are provided to illustrate how each of the steps can be done.

Step 1 – Risk Identification: Think about risks in the areas of Compliance, Financial, Operational, and Strategic. Risk identification means writing risk statements that are specific as to the nature of potential loss of harm, and that focus on root causes.

Step 2 – Risk Assessment: Users choose the level of assessment they wish to conduct, based on the types of qualitative and quantitative information and analysis, and the level of expertise they have available to participate. UW's standard scales for rating likelihood and impact of each risk statement are used to convert each risk into a level from "extreme" to "low" and produce a prioritized list of department risks.



Legend	Meaning
Extreme	Significant capability loss and the achievement of objectives is unlikely
High	Significantly degrades the achievement of objectives or capability
Substantial	Will degrade the achievement of objectives or capability
Medium	May degrade achievement of some objectives or capability
Low	Little or no impact on the achievement of objectives or capability

Users need to document what controls—such as policies and procedures, education and training, oversight, monitoring and audits—are currently in place, since these form the basis for the risk ratings.

Step 3 – Risk Mitigation: Users think about their top risks from the assessment step, and in light of current controls, what options can be considered to mitigate (i.e. to prevent a loss from occurring) the top risks. Mitigation is a forward looking activity that typically addresses four classic risk management options: avoid, reduce, transfer, or assume the risks. This results in a mitigation plan to manage or reduce risk to an acceptable level, identifying who is responsible and how results will be communicated.

Step 4 – Risk Communication and Monitoring: A risk assessment will be of little value if it sits on a shelf and there is no follow up to the risks identified (unless all the assessed risks are "low" in which case the user may want to consider if they are ***over-*** controlling their risks). Communicating and monitoring ensures that risks, controls, and mitigation plans are transparent and relevant for the department. Depending on the risks assessed, actual progress on mitigation plans may become part of the organization's performance measurement, management and reporting systems.

The ERM self-assessment toolkit is printed as a manual (copy available), and our goal is to share the self-assessment toolkit widely throughout the University, and with others in higher education. As users gain experience doing their own risk assessments, we look forward to sharing their results in future ERM reports.