UW Technology Enterprise Risk Assessment

Final Report

April 2009

Interim COO
Distributed Systems
Enterprise Platforms
Learning & Scholarly Technologies
Network Systems
Planning & Facilities Initiatives
State IT Relations
Technology Strategy & Architecture
Technology Services
UWTV

INTRODUCTION

This report is provided at the request of Kelli Trosvig, Interim COO of UW Technology. It consists of: 1) this introduction; 2) a summary of top risks; 3) a summary of top risk potential mitigation options; and 4) appendices containing supporting documentation (example risks, risk scores, charter, methodology).

The purpose of the exercise was to: a) conduct a risk assessment; b) inform UW leadership of key IT service risks, and c) guide UW Technology management in setting budget priorities.

ASSESSMENT TEAM

The risk assessment team consisted of:

Clare Donahue, Cris Ewell, Terry Gray (Chair), Alisa Hata, Kerry Kahl, Scott Mah, Sid McHarg, Tom Profit, Lori Stevens, Pam Stewart, and Karalee Woody.

KEY FINDINGS

The major risks to services provided by UW Technology fall into these three categories:

Data Security
Business Continuity
Strategic Positioning

The first two categories (data security and business continuity) were scored as HIGH risks, where HIGH is defined as "**Significantly degrades achievement of objectives or capability".** The third category (strategic positioning) was scored as SUBSTANTIAL, where that level is defined as "**Will degrade the achievement of objectives or capability".**

NEXT STEPS

A summary of this report showing top risks and potential mitigation options) will be presented to the President's Advisory Committee on Enterprise Risk Management.

Within UW Technology, these findings will inform our resource allocation and prioritization processes. However, in the current austere budget climate we may conclude that the university's tolerance for risk exceeds its capacity to fund risk mitigation projects, so difficult decisions will need to be made –and history suggests that tactical needs often take precedence over strategic risk mitigation. Nevertheless, there are important steps that can be taken within the current budget constraints by deferring less important projects. (One example would be to make the long-term remediation project for improving the security of Nebula desktop computers a top priority.)

UW Technology Investments – 2009 Risk Assessment

SUMMARY OF TOP RISKS

Risk Assessment Work Group:
Clare Donahue, Cris Ewell, Terry Gray, Alisa Hata, Scott Mah, Sid McHarg, Tom Profit, Lori Stevens, Pam Stewart, Karalee Woody

DATA SECURITY

Risk is "HIGH" – Significantly degrades achievement of objectives or capability

Disruption of one or more critical services due to cyberattack, compromise

Exposure, modification, or deletion of sensitive data

BUSINESS CONTINUITY

Risk is "HIGH" – Significantly degrades achievement of objectives or capability

Failure to resume operations promptly due to inadequate DRBC planning or execution

Disruption of major IT facility (with consequent critical service disruption) due to natural or man-made disaster (e.g. fire, hazardous materials); or due to necessary resources unavailable (e.g. power, water, staff)

Disruption of one or more critical services due to hardware damage/failure; or to inability to recruit/retain staff with required experience, expertise, and skills; or to insufficient resources to maintain, upgrade, or replace resources; or to inadequate policy, procedures, planning, controls

Fewer services available to campus due to external events reducing available dollars (many different sources, e.g. state/federal funding, vendor pricing)

Failure to perform deferred maintenance leads to costs of early system or facility replacement

STRATEGIC POSITIONING

Risk is "SUBSTANTIAL" – Will degrade the achievement of objectives or capability

Lack of technology vision results in missed opportunities for University research, teaching, learning

Missed opportunities for new, increased revenues; or for cost reductions

Highest Likelihood
Highest Impact
↕
Lowest Likelihood
Lowest Impact

Legend	Meaning
High	Significantly degrades the achievement of objectives or capability
Substantial	Will degrade the achievement of objectives or capability

Rating Validation: **INTERMEDIATE**. Excellent team expertise in all operational and technical areas of UW Technology, depth of experience providing services for the University. Good evidence of potential, current/real failures and impacts on services, and of current environment and capability/resiliency.

UW Technology Investments – 2009 Risk Assessment

SUMMARY OF TOP RISK POTENTIAL MITIGATIONS

Risks are "HIGH" – Significantly degrades achievement of objectives or capability

Risk Category A: *DATA SECURITY*

Operational 3.3: Disruption of one or more critical services due to cyberattack, compromise

Compliance 1: Exposure, modification, or deletion of sensitive data

A project is defined to address two of what we consider high-risk items from the long-term Nebula desktop remediation report. The purpose of this is to help mitigate a future *coreflood-type* event (see https://wiki.cac.washington.edu/x/44TZ)

Re-establish a security group, with CISO involvement, to identify and act on security priorities

Review servers with sensitive data - work with customers to consolidate servers and protect appropriately

Catalog and map assets with sensitive data to aid in incident response

Work with key vendors to reduce and/or transfer UW data security risks

Risks are "HIGH" – Significantly degrades achievement of objectives or capability

Risk Category B: *BUSINESS CONTINUITY*

Operational 5: Failure to resume operations promptly due to inadequate DRBC planning or execution

Operational 2.1/2: Disruption of major IT facility (with consequent critical service disruption) due to natural or man-made disaster (e.g. fire, hazardous materials); or necessary resources unavailable (e.g. power, water, staff)

Operational 3.2/6: Disruption of one or more critical services due to hardware damage/failure; or inability to recruit/retain staff with required experience, expertise, and skills

Operational 4.1/4: Degradation of one or more critical services due to insufficient resources to maintain, upgrade, or replace resources; or inadequate policy, procedures, planning, controls

Financial 3: Fewer services available to campus due to external events reducing available dollars (many different sources, e.g. state/federal funding, vendor pricing)

Financial 4: Failure to perform deferred maintenance leads to costs of early system or facility replacement

Proceed with planned Business Continuity scoping study and present the results to the Interim University Technology Advisory Committee (UTAC)

Replicate servers to location outside of Puget Sound seismic area and provide associated network connectivity

Conduct audit to ensure all critical infrastructure is supported

Invest in single-point-of-failure and service-dependency analysis on an ongoing basis

Develop processes and periodically execute tests to demonstrate capability, or provide a sufficiently resilient infrastructure to mitigate this problem

Develop policies and implement processes to ensure all data required to restore critical services are adequately maintained outside of Puget Sound seismic area

Add necessary components to support related non-mainframe processing needed to support core business systems, both from an application and infrastructure perspective

Focus on community engagement to identify services that must be cut due to insufficient resources

Distribute budgets and budget responsibility within UW Tech to help with equipment replacement and other planning

Encourage and enable training of technical staff, even in difficult times, in order to retain key staff members and help them stay current with technology

Implement tools and process for monitoring, responding to, and resolving failures and outages

Risks are "SUBSTANTIAL" – Will degrade the achievement of objectives or capability

Risk Category C: *STRATEGIC POSITIONING*

Strategic 2: Lack of technology vision results in missed opportunities for University research, teaching, learning

Financial 1/2: Missed opportunities for new, increased revenues; or for cost reductions

Purse the new revenue proposals identified in the Rapid Process Improvement effort

Continue to invest in two of the "Next Big Thing" areas: cloud computing and mobility

Develop IT strategic plans, with ongoing review and updates, and a culture of anticipation, innovation, and agility

Ensure we keep our staff up on new technologies by supporting training and R&D

Provide better communication with staff about strategic technology direction and priorities so staff can ramp up

Seek and maintain executive sponsorship for strategic engagements and collaborations, even if sometimes speculative

Highest Likelihood
Highest Impact ↕
Lowest Likelihood
Lowest Impact

Legend	Meaning
High	Significantly degrades the achievement of objectives or capability
Substantial	Will degrade the achievement of objectives or capability

UW Technology Investments – 2009 Risk Assessment

APPENDICES

- Appendix A - Top Risk Examples and Current Controls
- Appendix B - Risk Statements by Risk Category
- Appendix C - Risk Statements by Score
- Appendix D - Charter
- Appendix E - Methodology

Appendix A

UW Technology Investments – 2009 Risk Assessment

TOP RISK EXAMPLES & CURRENT CONTROLS

Risk Category A: *DATA SECURITY*

--> Risk is "HIGH" – Significantly degrades achievement of objectives or capability

Operational 3.3: Disruption of one or more critical services due to cyberattack, compromise

Compliance 1: Exposure, modification, or deletion of sensitive data

Examples of failures/impacts "horror stories" – "what keeps you up at night" [our own-peers-industry]

A cyber attack of some type brings down key UW Technology services, severely impacting the work of the University

- Actual Example: Last year the Coreflood virus affected numerous administrative users who were unable to access their Nebula systems for multiple days resulting in lost productivity
- Hypothetical Example: Exploit of previously unknown Cisco bug or of weak/known UW router passwords results in flooding the network making it unusable (and impossible to troubleshoot remotely)
- Hypothetical Example: Compromise of Red Hat Linux operating system (while not as likely as Windows) causes malicious deletion of email folders and/or inability to access disk shutting down access to our email servers and requiring days and days to restore folders from backups

Exposure of sensitive data

- Hypothetical Example: Security breach of payroll data transmittal results in exposure of SSNs
- Hypothetical Example: Security breach results in exposure of email related to budget planning

Lab workstations are unavailable due to virus

Student data could be lost due to malicious code in public space

Catalyst Web Tools database servers contain a variety of private data: student data, Human Subjects/UW IRB-compliant research data, patient data, etc.

Husky card point of sale or parking system compromise resulting in exposure of names and SSNs

Cyber attack and successful breach of Blackberry Enterprise Development Server that allowed stepping stone attacks of production environment. Breach detected prior to production compromise. If compromise occurred, senior executive email, calendars, and contacts would be exposed

Compromise of UW NETID accounts resulting in outbound email spamming and unauthorized access to UW library resources

Our physical security practices are inadequate. These were pointed out in the 2004 "Data Center Security Master Planning Study" done by Callison. We have inconsistent staffing of the badge issuing function and no way of monitoring the revolving door practice of folks entering the data center, i.e. holding the doors open for others who may or may not be credentialed

Current environment/capabilities – What controls are in place, what plans and mitigations

Here is a partial list of what we currently do for our server environment in UW Technology to help keep them secure:

- We do regular patching of servers
- Professional staff keep up with security issues via talking to one other, reading lists, notices from vendors, etc.
- We ensure that all code that should be the same is but distributing software to many of our servers regularly.
- We only enable ports and services that should be enabled
- We keep up with SPAM and anti-virus software

And more, including: Tipping point, application security support, network traffic filtering (AV and Spam), and network ops center

Risk Category B: *BUSINESS CONTINUITY*

–> Risk is "HIGH" - Significantly degrades achievement of objectives or capability

Operational 5: Failure to resume operations promptly due to inadequate DRBC planning or execution

Operational 2.1/2: Disruption of major IT facility (with consequent critical service disruption) due to natural or man-made disaster (e.g. fire, hazardous materials); or necessary resources unavailable (e.g. power, water, staff)

Operational 3.2/6: Disruption of one or more critical services due to hardware damage/failure; or inability to recruit/retain staff with required experience, expertise, and skills

Operational 4.1/4: Degradation of one or more critical services due to insufficient resources to maintain, upgrade, or replace resources; or inadequate policy, procedures, planning, controls

Financial 3: Fewer services available to campus due to external events reducing available dollars (many different sources, e.g. state/federal funding, vendor pricing)

Financial 4: Failure to perform deferred maintenance leads to costs of early system or facility replacement

Examples of failures/impacts "horror stories" – "what keeps you up at night" [our own-peers-industry]

Chronic water Leakage in the 4545 parking garage is damaging equipment in the datacenter below. A meeting was held with Commuter Services to discuss, but a solution is still a ways off. Water has also migrated to the outside wall and part of the ceiling is rusting

Network Router Centers-experiencing water leaks (Chemistry Building the most recent example) and a number of them are in need of HVAC upgrades/replacement. We also lack accurate monitoring systems for these facilities, e.g. we need to extend our BMS (building management system) to these locales

Lack of preparation for a regional disaster results in an inability to respond in a reasonable way to bring up critical services and help other units resume the business of the university

- Actual Examples (of regional natural disasters and universities): Tulane and Katrina, University of Iowa and June 2008 flooding, Cal state and Northbridge earthquake, UW and Nisqually
- Hypothetical Example: A terrorist attack in Seattle injures thousands, flooding Harborview and UWMC with patients, and disrupts power and Internet connectivity; UW Technology is unable to get techs on site to the hospitals, the Westin, or most router centers; network connectivity and phone service is severely disrupted, and UW Technology has neither the staff nor the plans to put alternative communication technologies in place
- Hypothetical Example: Pandemic results in thousands of UW faculty, students, and staff attempting to work and study at home, overwhelming services such as weblogin, Catalyst tools, email, web conferencing, and phone systems, and UW Technology doesn't have staff or plans in place to deal with increased volumes

A number of us believe that Business Continuity has not been more than lip service at UW, with potentially disastrous consequences, perhaps because the cost of "good" BC is significant

1) There appears to be no general policy regarding Business Continuity on this campus
    a. Not even for a segment of the Apps like those supported by OIM
    b. Not even for any portion of infrastructure such as the network, data center or the systems within the data center
2) There seems to be no interest in such a policy (not to be confused with life safety and initial response) . We can't even find enough interest to have the complete conversation within our own organization, nor even enough to understand how the subject is being addressed across our own variety of apps, middleware, and physical infrastructure
3) We appear to be adopting some of the virtualization technologies and exploiting them for the benefits that might be offered to allow engineers to manage the patch process easier but to no other benefit
4) We can live (and sleep) with a policy that clearly states the UW policy (whatever it is). It's the lack of a policy that is of concern. If there were to be a policy, it should be funded; and maybe address some of the assertions below
    a. Critical services should be supported by a demonstrated ability to continue to process without transaction loss during/after a natural or other event that might disrupt essential institutional services
    b. Today's "best of breed" applications, at best, provide piece-meal BC solutions; whereas a more systemic and comprehensive approach would be advantageous
    c. Assuming that 'recovery' of any design works without testing represents a big risk

The lack of a demonstrated capacity to restore our critical infrastructure in a consistent manner from information maintained outside of the Puget Sound area has not been adequately communicated outside of UW Technology and represents a considerable vulnerability should a regional disaster occur

Major incident affecting UW tunnel system, causing significant damage to key utilities and communications infrastructure

Westin Building failure or catastrophic damage affecting regional connectivity and significant UW infrastructure (in particular, the PNWGP –Pacific Northwest GigaPOP)

Widespread regional power disruption (duration greater than a single business day)

Major disruption to Puget Sound transportation/roadways affecting ability to get essential staff to/from key service locations

If OUGL or other student labs were no longer be available, due to some disaster, the ability to support student academic needs would be reduced

A wide variety of software services and applications are crucial to UW's mission, and any incidents disabling or degrading those services could have significant impact on UW operations. Examples include email, web publishing, Catalyst tools, etc.

A local or regional event that affected the ability of UW Technology staff to perform their job functions could quickly put critical IT services at risk

Similarly, insufficient resources (especially staff) could adversely affect business continuity objectives

Several resource issues affect service delivery and business continuity, both directly and indirectly. Some examples follow

Campus Building Infrastructure-there are still many buildings on the UW campus that suffer from lack of communications infrastructure to support current/needed bandwidth technology. The plan and the will are there, but the funding is unreliable

Lack of funding for staffing causing reduction in hours available for client support causing longer response times

Older Equipment Replacement-we have no replacement mechanism in place for older equipment/infrastructure, some of are at or beyond the end of useful life, e.g. in ACC the chiller and fan coils are 40 years old and the UPS (Uninterruptable Power Supply) is 30 years old; in 4545 we have a cooling tower and some CRACs (Computer Room Air Conditioner) and UPS that are 30 years old). In addition some elements, like our type of raised floor, are no longer made, making replacement difficult if not impossible. Our fire suppression system is still halon, which contains the CFC's that have been outlawed

Deferred Maintenance-some of the items identified in the pre-ESCO (Energy Services Company) study of the 4545 building have still not been addressed, e.g. seismic enhancements, sump pumps

Lack of resources results in deferring maintenance, replacement of equipment, or training, causing extended outages and much higher costs in the future

- Hypothetical Example: Less attention to building maintenance and to training staff who monitor facilities results in flooding of the sub-basement power vault, a complete 4545 data center outage, and days of mop up and repair (Imagine the failed water fountain valve on the 4545 4th floor, Mother's Day 2008, -- an actual example -- on a grander scale where city water comes into the building and no one on site knows how to shut it off)
- Hypothetical Example: Staff shortages due to resource constraints don't allow time for cross training or depth of coverage in critical areas resulting in extended outages (Pick your favorite critical application, say weblogin, and imagine it failing while one person on vacation and another comes down with pneumonia)

Current environment/capabilities - What controls are in place, what plans and mitigations

We have a Chief Technology Architect in place who keeps up on technology strategy

We have plans for more virtualization and making sure we are using the best solution

We have plans for cloud computing involving multiple vendors and multiple services

We have engaged key cell phone providers in strategic mobile communication partnerships

Highest Likelihood
Highest Impact ↑

Lowest Likelihood
Lowest Impact ↓

Legend	Meaning
High	Significantly degrades the achievement of objectives or capability

Appendix B

UW Technology Investments – 2009 Risk Assessment

RISK STATEMENTS BY RISK CATEGORY

OPERATIONAL RISKS

Disruption of entire region (with consequent critical service disruption) due to:

O1.1 → natural or man-made disaster (e.g. fire, hazardous materials)

O1.2 → necessary resources unavailable (e.g. power, water, staff)

Disruption of major IT facility (with consequent critical service disruption) due to:

O2.1 → natural or man-made disaster (e.g. fire, hazardous materials)

O2.2 → necessary resources unavailable (e.g. power, water, staff)

Disruption of one or more critical services due to:

O3.1 → software malfunction

O3.2 → hardware damage / failure

O3.3 → cyberattack / compromise

O3.4 → undetected system flaw (design or implementation)

O3.5 → vendor failure

O3.6 → inability to recruit and retain staff with required experience, expertise and skills

Degradation of one or more critical services due to:

O4.1 → insufficient resources to maintain/upgrade/replace/etc

O4.2 → unanticipated growth in demand (capacity meltdown)

O4.3 → insufficient clarity re who can make decisions to fix a problem

O4.4 → inadequate policy, procedures, planning, or controls

O5. Failure to resume operations promptly due to inadequate DRBC planning or execution.

COMPLIANCE RISKS

C1 Exposure, modification, or deletion of sensitive data

C2 Failure to meet federal, state, or local compliance requirements for data and infrastructure management such, as retention rules.

C3 Inability to respond to legal orders, for example eDiscovery

FINANCIAL RISKS

F1 Missed opportunities for new or increased revenues

F2 Missed opportunities for cost reductions

F3 Fewer services available to campus due to external events reducing available dollars (many different sources, e.g. state/fed funding, vendor pricing.)

F4 Failure to perform deferred maintenance leads to costs of early system or facility replacement.

STRATEGIC RISKS

UW's technology does not keep up with:

S1.1 → innovations/user needs and expectations, resulting in diminished national reputation and disadvantage when compared with peer institutions

S1.2 → capacity needs, thus limiting UW's ability to compete for new programs, eg. major research funding opportunities

S2 Lack of strategic technology vision results in missed opportunities for next-generation research, teaching, and learning on a global, 24x7 scale

S3 Inability to leverage wisdom and experience of peer institutions, shape the technology marketplace, and promote the reputation of UW, because budget and travel restrictions preclude participation in national/international tech discussions

S4 Loss of trust by campus, due to management failures, precludes successful IT strategy

Appendix C

UW Technology Investments – 2009 Risk Assessment

RISKS RANKED BY SCORE

TOP RISKS

Operations:	Cyberattack, compromise O3.3	15.6
Compliance:	Exposure, modification, deletion of sensitive data C1	11.9
Financial:	External events reduce funding, fewer services available for campus F3	12.55
Operations:	Major facility disruption due to natural or man-made disaster O2.1	11.6
Operations:	Major facility disruption due to resources unavailable (power, water, staff) O2.2	11.1
Operations:	Failure to resume operations due to inadequate DRBC planning, execution O5	10.8
Operations:	Critical service disruption due to Inability to recruit/retain staff O3.6	11.4
Financial:	Failure to perform maintenance leads to early system/facility replacement costs F4	10.55

NEXT RISKS

Operations:	Disruption of one or more critical services due to hardware damage/failure O3.2	10.2
Operations:	Degradation of one or more critical services due to insufficient resources to maintain, upgrade, replace O4.1	10.2
Operations:	Degradation of one or more critical services due to inadequate policy, procedures, planning, controls O4.4	9.8
Strategic:	Lack of technology vision results I missed opportunities for University research, teaching, learning S2	10.0
Financial:	Missed opportunities for new, increased revenues F1	10.0
Financial:	Missed opportunities for cost reductions F2	9.6

LOW RISKS	
Operations: Disruption of one or more critical services due to software malfunction O3.1	9.1
Operations: Disruption of entire region/critical service disruption due to necessary resources not available O1.2	8.9
Strategic: Loss of campus trust due to mgt failures, precludes IT strategic success S4	8.9
Strategic: UW technology does not keep up with capacity needs, limits ability to compete for new programs/funding S1.2	8.7
Strategic: Unable to leverage wisdom/experience of peers, shape tech marketplace due to lack of participation in national/international forums S3	8.5
Strategic: UW technology does not keep up with innovations/user needs, diminishes reputation and at disadvantage compare to peers S1.1	8.1
Compliance: Fail to meet fed/state/local requirements for data/infrastructure mgt, eg. retention rules C2	7.9
Operations: Disruption of entire region/critical service disruption due to natural/manmade disaster O1.1	7.3
Operations: Disruption of one or more critical services due to vendor failure O3.5	7.1
Operations: Disruption of one or more critical services due to vendor failure O3.5	6.6
Operations: Disruption of one or more critical services due to undetected system flaw O3.4	6.4
Compliance: Inability to respond to legal orders, eg. eDiscovery	6.0
Operations: Degradation of one or more critical services due to unanticipated demand growth/ capacity meltdown O4.2	4.9

Highest Likelihood
Highest Impact

Lowest Likelihood
Lowest Impact

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

Appendix D

UW Technology Investments – 2009 Risk Assessment

CHARTER

Date: Fri, 16 Jan 2009 08:29:00 -0800 (Pacific Standard Time)
From: Terry Gray <gray@washington.edu>
Subject: Re: Risk assessment for UW Technology

WELCOME

Thank you for being willing to particpate in this activity. Each of you bring unique knowledge and judgment in a broad range of areas which we need to integrate for this exercise, so all of your inputs are essential to the success of this assignment. I know that everyone is trying to do the work of many right now, so we'll try to keep this new task as constrained as possible.

CHARGE

Kelli wrote:

"As we worked on the extension of our Unisys agreement and the replacement of data storage systems at the end of last year, I felt that having a risk assessment done for UW Technology in general will provide a valuable perspective as part of our long term planning. The year-end snow storms and flooding in our data center illustrate and emphasize our risk exposures. Terry Gray has started to work with Kerry Kahl on identifying major risks, and we want to have you participate in refining the set of risk statements, then assessing them using the ERM process. I will also ask Kirk Bailey to have one of his IT security staff participate.

This is expected to be a quick review, no more than three or four meetings of 90 minutes each. I have asked Terry to serve as team leader, and Kerry will be ERM facilitator. I would like to have your assessment by the end of February; Juniper will work on getting these meetings scheduled."

Separately, Kelli has emphasized to me the importance of using this process to help inform planning and investment decisions for our remote site at Tierpoint.

GOALS

The overall objective is to identify the biggest risks to the most critical services provided by UW Technology, and suggest mitigations for them. More specific goals are to:

1) Using methodology from UW's risk mgt group, prioritize IT risk areas among the broad categories listed in the attached document. As you review the candidate risk statements, you'll see that they do not distinguish individual services, some of which are more important to UW than others. The idea is to start by understanding the "big picture" exposures, e.g. how vulnerable we are to operational failures, as compared to compliance, or financial, or other risks. However, we also need to…

2) Identify examples and anecdotes of specific high-impact services that are at risk, and ideas for how to mitigate the risk. And finally…

3) Identify a preliminary list of services/capabilities/infrastructure that should be considered a high priority for replication at a remote site (such as Tierpoint in Spokane.)

NON-GOALS

1) A full-on detailed risk analysis of all of our services, with each service prioritized.

2) Analysis of administrative *applications* --however, the platforms and supporting infrastructure *for* the administrative apps are very much in-scope; indeed, one of the primary drivers for this exercise.

DELIVERABLE

A report to Kelli that covers the three goals above, starting with the output from a computer-assisted risk assessment exercise and augmented with our examples of key concerns and potential mitigations.

Appendix E

UW Technology Investments – 2009 Risk Assessment

METHODOLOGY

Within the standard risk categories of Operational, Compliance, Financial, and Strategic, a series of "risk statements" was developed, such as: "Exposure, modification, or deletion of sensitive data". Each of these was then rated by the team for "Likelihood" and "Impact". Those that scored highest (by summing each team member's Likelihood and Impact scores, then taking the average values) were then eventually grouped together into three major categories of risk.

For each major risk category, examples were identified, along with current controls, and possible mitigations.

In order to validate the results of voting on individual risk statements, and to help group those statements, the following exercise was conducted: Team members were asked to write on a card the top three categories of risk that "kept them up at night". We then compared notes, and found that everyone had included data security and business continuity. For the third choice, the group was split between strategic positioning (or lack thereof) and insufficient resources.

We observed that the insufficient resources risks were aspects of the other categories, especially Business Continuity. We thereby settled on data security, business continuity, and strategic positioning as our top three risk categories, and then organized the risk examples and mitigation options into those three groups.