Risk Management Guide

November 2016

**Office of Environmental, Health, Safety
and Risk Management
The City University of New York
205 East 42nd Street
New York, NY 10017
(646) 664-2854
ehsrm@cuny.edu
www.cuny.edu/risk**

Table of Contents

Environmental,
Health,
Safety and
Risk Management

The City University of New York
Standard Operating Procedure
Risk Management Guide
November 2016

List of Figures

Introduction

Dear Risk Management Colleagues,

In a July 2007 memo addressed to college presidents, Allan H. Dobrin, Executive Vice Chancellor and Chief Operating Officer of The City University of New York (CUNY), announced the creation of a dedicated CUNY risk management function. The change reflected an increasing awareness that CUNY, like most of the nation's universities, should have a comprehensive risk management program to mitigate liability in all areas of University activity.

Each campus has created a Risk Management Committee that is responsible for developing and implementing a comprehensive Risk Management Plan to identify, assess, and mitigate the institution's risks. This Risk Management Guide (RMG) and its supplemental templates provide the framework for that Plan.[*]

Please check the Environmental, Health, Safety and Risk Management (EHSRM) SharePoint website (https://ehsrm.cuny.edu/riskmanagement/default.aspx) to be sure that you have the most recent version of this Guide and to access supplemental information. In addition, we welcome your input and comments, so that we may continue to improve the University's risk management program.

Sincerely,

Howard N. Apsan, Ph.D.
University Director
Environmental, Health, Safety and Risk Management
The City University of New York
205 East 42nd Street
New York, NY 10017
+1.646.664.2854
howard.apsan@cuny.edu

"A good hockey player plays where the puck is. A great hockey player plays where the puck is going to be."
–Wayne Gretzky

---

[*]This Guide is not intended to supersede any specific operational rules or procedures that have been adopted by the University to comply with health, safety or other regulations or policies. This Guide is a compilation of ideas from various sources and we acknowledge their contributions in our Resources page. We would like to extend special thanks to the University of Washington for their particularly helpful contribution.

The Risk Management Process

The four steps of the risk management process are:

Step 1 – Risk Identification
Step 2 – Risk Assessment
Step 3 – Risk Mitigation
Step 4 – Risk Communication
     & Monitoring
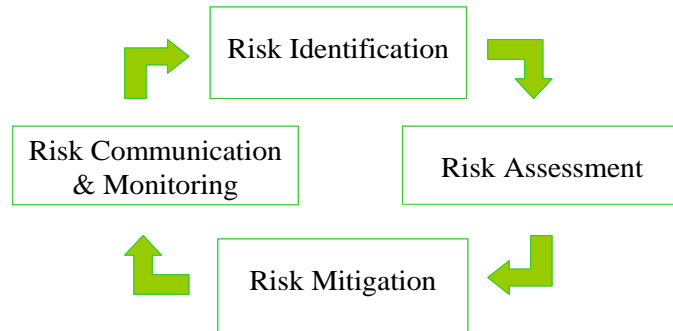
Risk management is intended to identify opportunities for mitigation and strengthen the existing CUNY efforts by providing a standardized process, access to information (e.g., resources, newsletters) and access to effective tools (e.g., risk maps, metrics and self-assessment approaches). A comprehensive risk management process will**:**

- ➢ assign a cross-functional group to identify risks;
- ➢ prioritize risks;
- ➢ sift through the prioritized risks to decide which ones require immediate attention;
- ➢ develop a Risk Management Plan;
- ➢ re-assess priority risks at least once a year; and
- ➢ be an iterative process.

Risk Types

To help guide our discussion of risks, The National Association of College and Business Officers (NACUBO) has identified five risk types in higher education institutions:

1. **Compliance Risk:** Risk created by failing to follow federal, state or local law, regulation or University policy or procedure that safeguards the University from legal exposure.
2. **Financial Risk:** Risk that may result in loss of physical assets or financial resources.
3. **Operational Risk:** Risk that affects ongoing day-to-day management processes.
4. **Strategic Risk:** Risk that affects the University's ability to achieve its objectives.
5. **Reputational Risk:** Risk that affects the perception that others have of the University.

Broad Risk Areas Defined

Based on previously submitted Campus Risk Management Plans, the following functional areas should be considered in the risk management process.

Academic Affairs - Provides assistance, leadership, guidance and resources to the entire academic division.

Buildings and Grounds - Oversees building maintenance, repair and upgrades, and complies with environmental, safety and health procedures relating to facility operations. Buildings and Grounds controls and supervises utilities, equipment, and all custodial services.

Business Continuity - Ensures that critical business functions will be available to customers, suppliers, regulators, and other entities that must have access to those functions. Business Continuity refers to those activities performed daily to maintain service, consistency, and recoverability.

Computer and Information Services – Manages the use of computers and telecommunications to retrieve, store, and transmit information.

Environmental Health and Safety - Manages and oversees all environmentally related activities on campus. Environmental Health and Safety refers to environmental compliance, policy, waste management and training activities as well as lab safety, research, audits, permits, and chemical management. Also is responsible for illnesses, immunizations, communicable disease spreading and any other biological risks.

Budget and Financial - Provides accounting and financial management systems in accordance with CUNY statutes. Finance manages cash and investments, fixed assets, debts, endowments, grants, payroll and timekeeping, and procurement of goods and services.

Human Resources – Manages staffing, operation, organization, compensation, hiring, employee performance management, organization development, administration, and training.

Public Safety – Serves to prevent and protect the University from emergency events and incidents that may cause significant danger, injury, damage, or harm.

Student Services - Provides services and support for students to enhance student growth and development. It encompasses developing programming, advising student organizations and student leaders, student conduct, athletics, financial aid, career development, enrollment management, and study abroad.

Step 1 – Risk Identification

Common approaches used to identify risks include interviews, personal inspections, and a review of pertinent documents. Risk identification provides the foundation for the risk management process and may involve the input of a cross-functional and diverse Risk Management Committee.

Documenting Risk Identification

PURPOSE: To identify specific risks for a broad risk area.
GOAL: Reveal subject risk areas and identify risk statements for a broad risk area.
HOW TO DOCUMENT RISK IDENTIFICATION: After reviewing Step 1, generate subject risk areas and risk statements for each broad risk area. Use plain language and be specific.

Broad Risk Area: Pollution

SUBJECT RISK AREAS	RISK STATEMENTS
1. Air quality (fires/smoke, toxins, second hand smoke, fume hood exhaust)	Air emissions exceed Air Operating Permit (AOP) limits.
2. Electronic equipment/computers/ batteries	Large waste stream with little or no disposal options.
3. Permits and licenses	Revocation of radioactive materials license.
4. Security	Unauthorized access or use of restricted materials.

Figure 1: Example – Risk Identification Worksheet

Step 2 – Risk Assessment

The goal of Step 2 is to prioritize your risks, which involves assessing the likelihood of occurrence and the potential impact. To complete this risk assessment, document the assigned measure of likelihood and impact for each risk statement. Members of the Risk Management Committee may be provided with the following tables to serve as references for the assessment.

Likelihood of Occurrence: Likelihood (e.g., probability or frequency) may be determined by using a scale of 1 – 5.

Rank		Measures of Likelihood
1	Rare	May only occur in exceptional circumstances (e.g., less than once in 10 years).
2	Unlikely	Could occur at some time (e.g., at least once in 10 years).
3	Possible	Might occur at some time (e.g., at least once in 5 years).
4	Likely	Will probably occur (e.g., at least once per year).
5	Almost Certain	Expected to occur in most circumstances (e.g., more than once per year).

Figure 2: Measures of Likelihood

Impact of Occurrence: Impact (e.g., consequence or severity) is determined by using a scale of 1 – 5. When an event has multiple impacts, select the most severe (i.e., highest number) for the measure of impact.

Rank		Measures of Impact				
		Injuries	Financial Loss (underdevelopment)	Asset Loss	Interruption of Services	Reputation and Image
1	Insignificant	No injuries	<$1M or <1% of Budget	Little or no impact on assets	< ½ day	Unsubstantiated, low impact, low profile or no news items
2	Minor	First aid treatment	$1M - $10M or 1% of Budget	Minor loss or damage to assets	½ - 1 day	Substantiated, low impact, low news profile
3	Serious	Medical treatment	$10M - $20M or 2% of Budget	Major damage to assets	1 day - 1 week	Substantiated, public embarrassment, moderate impact, moderate news profile
4	Disastrous	Death or extensive injuries	$20M - $50M or 6% of Budget	Significant loss of assets	1 week - 1 month	Substantiated, public embarrassment, high impact, high news profile, third party actions
5	Catastrophic	Multiple deaths or severe permanent disabilities	>$50M or >6% of Budget	Complete loss of assets	> 1 month	Substantiated, public embarrassment, very high multiple impacts, high widespread news profile, third party actions

Figure 3: Measures of Impact

Documenting Risk Assessment

PURPOSE: To assess risk statements and classify them according to risk types.
GOAL: Identify the NACUBO risk types (see page 4) associated with each risk statement, and the impact and likelihood of each risk. Identifying this information in a single chart will help determine risk prioritization.
DOCUMENT RISK ASSESSMENT: See the template below.

Risk Statement	Risk Types (check one or more)						Department(s) Affected	Impact	Likelihood
	Operational Risk	Financial Risk	Compliance Risk	Strategic Risk	Reputational Risk	Other Risk			
Air emissions exceed air operating permit			X				Environmental Health and Safety	3	2

Figure 4: Example – Risk Assessment Template

CU NY Environmental,
Health,
Safety and
Risk Management

The City University of New York
Standard Operating Procedure
Risk Management Guide
November 2016

Risk Map: Likelihood and impact are multiplied to produce a visual array of risk levels. Risks that plot in the upper right corner are considered "chief risks" and should receive priority over those that plot towards the bottom left.

Catastrophic	5	5	10	15	20	25
Disastrous	4	4	8	12	16	20
Serious	3	3	6	9	12	15
Minor	2	2	4	6	8	10
Insignificant	1	1	2	3	4	5
IMPACT		1	2	3	4	5
	LIKELIHOOD	*Rare*	*Unlikely*	*Possible*	*Likely*	*Almost Certain*

Figure 5: Risk Map

Highest Likelihood
Highest Impact

Lowest Likelihood
Lowest Impact

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

Figure 6: Risk Levels Defined

Once a risk assessment has been completed, use the Risk Map to assist in prioritizing your risks, and then list them in the Chief Risks Chart.

Documenting Chief Risks

PURPOSE: To prioritize risks from highest to lowest.
GOAL: Rank chief risks and identify which ones should receive priority attention in the mitigation process.
HOW TO DOCUMENT CHIEF RISKS: After reviewing Step 2, select your institution's chief risks and rank them (with number 1 being the highest priority, or most "extreme" risk).

Priority (1=highest)	Risk	Risk Level (Impact x Likelihood)	Notes
1	Lab fire	25	Lab fires may occur overnight or on weekends and may have serious impact.
2	Basement flooding	15	The campus is located in a flood zone. Flooding regularly occurs during heavy rain events, and electronic equipment is vulnerable.

Figure 7: Example – Chief Risks Chart

Step 3 – Risk Mitigation

Risk mitigation refers to the broad range of actions to prevent a loss from occurring or to respond to losses that have already occurred. Risk mitigation utilizes existing internal controls designed to mitigate risks, and identifies control measures that should be implemented.

Internal and Potential Controls

The following is a list of control measures that may be implemented during the risk mitigation phase:

1. **Policies and Procedures**
   Policies are rules established to reduce risk. Procedures are instructions that outline a series of steps taken to ensure that policies are followed.

2. **Education and Awareness Training for Students, Staff, and/or Faculty**
   Methods used to periodically inform job-specific training or orientation for new employees and in-service training for all employees.

3. **Operational Controls (Engineering and Administrative Controls)**
   Operational controls are mechanisms to confirm that a policy or procedure is followed. Operational controls include engineering and administrative controls. Engineering controls are built-in measures (e.g., access controls such as keys, door locks, and computer passwords). Administrative controls refer to organizational or work practice measures.

4. **Oversight, Monitoring or Executive Controls**
   These controls refer to those designated to verify (e.g. through tracking, inspecting, documenting, and interviewing) that controls are effective.

5. **Audit Controls**
   Formal methods employed to analyze compliance. Audits may include the analysis of documents and sampled transactions.

Environmental, Health, Safety and Risk Management

CU NY

Documenting Risk Mitigation

PURPOSE: To list existing internal controls and design potential controls.
GOAL: To identify gaps in existing internal controls and brainstorm potential controls to address those gaps.
HOW TO DOCUMENT RISK MITIGATION: After reviewing Step 3, list existing internal controls for a specific risk and then brainstorm and list potential controls that could be put in place to address remaining risk.

Subject Risk Area: Environmental Health and Safety
Risk Statement: Lab fires that jeopardize student and staff safety

Existing Internal Controls (those that are already in place)			
Control	**Description of Control**	**Type of Control**	**Notes**
Sprinkler System	Sprinkler systems are installed in all the labs and are set off when there is excessive smoke or fire.	Operational (Engineering)	Sprinklers can lead to water damage of other areas. Must be checked regularly.

Potential Controls (those that should be put into place)					
Control	**Description of Control**	**Type of Control**	**Cost**	**Timeline for Implementation**	**Notes**
Manual on mixing hazardous chemicals	Guidelines on which chemicals can and cannot be mixed together.	Education Awareness	Two hours per lab for EHS officer to teach guidelines.	2-3 weeks	

Figure 8: Example – Risk Mitigation Worksheet

Step 4 – Risk Communication & Monitoring

The next step in the risk management process is risk communication and monitoring. Communicating and monitoring is essential to ensure that risks, internal controls, and mitigation plans remain transparent and relevant, and it provides a feedback loop for improving mitigation plans.

When factors that affect the likelihood and impact change, those selected risks should be reassessed and reprioritized to foster continuous improvement of the risk management process.

Risk communication and monitoring plans should include the following:

➢ designate a risk owner to be responsible for each chief risk;
➢ minimize internal control gaps, overlap and errors;
➢ make risk and controls more transparent by providing immediate feedback; and
➢ Eliminate process redundancies unless deemed necessary for business continuity and/or disaster recovery reasons.

Annual Risk Mitigation Plan

An Annual Risk Mitigation Plan (Fig. 8) is a tool that documents the risk response and follow-up actions. In a uniform manner, it documents the risk, its impact and likelihood, existing internal controls, potential controls, communication, and monitoring plans for significant risks. Ideally, The Risk Mitigation Plan should be reviewed and updated at the same time each year.

CUNY Environmental, Health, Safety and Risk Management

Documenting Annual Risk Mitigation Plan

PURPOSE: To organize and evaluate existing internal and potential controls and establish communication and monitoring protocols.
GOAL: Reveal gaps in existing internal controls and evaluate potential measures that can be taken to mitigate each risk. Create communication and monitoring measures for follow-up purposes.
HOW TO DOCUMENT CONTROLS: After completing Step 3 and reviewing Step 4, document both planned risk mitigation and risk communication and monitoring strategies.

Risk Reference	Risk Identif-ication Risk Area: Risk Statement	Baseline (Without Mitigation)		Existing/ Potential Controls	Risk Mitigation						With Mitigation (Existing and Potential Controls)		Risk Communication and Monitoring			
		Likelihood	Impact		Policy and Procedures	Education and Awareness Training	Operational Controls	Oversight, Monitoring or Executive Controls	Audit Controls	Other Controls	Likelihood	Impact	Responsible Person	Time Line	Cost of Mitigation	Scheduled Date to Revisit Plan
Ex	**Chemistry Labs**: lack of guidelines endangers students	4	3	Existing Controls	Staff need to do X as outlined in Y	Policies and procedures are explained during…	Protocols are X, Y, and Z	Supervisor reviews … for accuracy and completeness	Labs are audited every 3 years		1	1	Mr. Jones	3 weeks	Training = $65 per employee plus labor costs	06/28/14
				Potential Controls	Staff must follow new guide-lines	Staff will be required to attend mandatory orientation	New guidelines and insurance policy will be set by external party X…	Mr. Jones reviews supervisor's review for accuracy and completeness	Labs will be audited every 2 years							

Figure 9: Example – Annual Risk Mitigation Plan

APPENDIX

Commonly Found Risks in Higher Education Settings
For a more comprehensive list of risks please see "Today's Campus" at
www.todayscampus.com/articles/load.aspx?art=1724.

Broad Risk Area: Auxiliary Enterprises
Subject Risk Area:
- Inadequate facilities maintenance
- Inadequate physical safeguards
- Theft of revenue or inventory
- Unhealthy/unsafe environment
- Shortage of trained personnel

Broad Risk Area: Financial Management
Subject Risk Area:
- Improper calculation and refunding of tuition and fees
- Breach of student confidentiality laws
- Failure to log checks as they are received
- Failure to ensure physical security of business office operations
- Inaccurate or untimely financial reports (SED, Comptroller's Office, GASB, etc.)

Broad Risk Area: Information Technology
Subject Risk Area:
- Business requirements and IT opportunities are not adequately considered
- Failure to maintain a business continuity and disaster recovery system
- Failure to market technology initiatives

Broad Risk Area: Physical Plant
Subject Risk Area:
- Failure to respond timely and correctly
- Inadequate training of staff
- Destruction of property
- Outdated or inefficient equipment

Broad Risk Area: Student Services
Subject Risk Area:
- Failure to safeguard confidential information
- Failure to obtain proper licensing and accreditation
- Failure to communicate health services information

CU NY Environmental,
Health,
Safety and
Risk Management

The City University of New York
Standard Operating Procedure
Risk Management Guide
November 2016

Risk Management Resources

Cassidy, D., Goldstein, L., Johnson, S., Mattie, J., Morley, J. (2001) *Developing a Strategy to Manage Enterprise-Wide Risk in Higher Education.* National Association of College and University Business Officers and Association of Governing Boards and PricewaterhouseCoopers. Copy available online at: http://urauthoring01.cuny.edu/main/wp-content/uploads/sites/4/page-assets/about/administration/offices/ehsrm/risk/nacubo_rm.pdf

Crowe Horwath and National Association of College and University Business Officers (2009) *Risk Assessment Standards Toolkit.* Copy available online at: http://www.nacubo.org/Documents/business_topics/Risk_Assessment_Toolkit.pdf

Gallagher, A. & Co. (2009) *Road to Implementation: Enterprise Risk Management for Colleges and Universities.* Arthur J. Gallagher Risk Management Services, Inc. Copy available online at: http://www.ajgrms.com/portal/server.pt/gateway/PTARGS_0_28406_570311_0_0_18/ERM%20TT%20Report%20Final%209-23-09.pdf

Mattie, J. et al. (2007) *Meeting the Challenges of Enterprise Risk Management in Higher Education.* National Association of College and University Business Officers and Association of Governing Boards. Copy available online at: http://www2.cuny.edu/wp-content/uploads/sites/4/page-assets/about/administration/offices/ehsrm/risk/NACUBOriskmgmtWeb.pdf

University Business Executive Roundtable. (2008) *Implementing Enterprise Risk Management.* The Advisory Board Company. Copy available online at: http://www2.cuny.edu/wp-content/uploads/sites/4/page-assets/about/administration/offices/ehsrm/risk/Implementing-Enterprise-Risk-Management.pdf

University Business Executive Roundtable. (2012) *A Practical Approach to Institutional Risk Management.* The Advisory Board Company. Copy available online at: http://www2.cuny.edu/wp-content/uploads/sites/4/page-assets/about/administration/offices/ehsrm/risk/25260_A-Practical-Approach-to-Institutional-Risk-Management.pdf

Unks, R. (2016) *Implementation Plan for Maricopa Integrated Risk Assessment Project at the Maricopa Community College District.* Maricopa Community Colleges. Copy available online at: http://www.maricopa.edu/mira/pdfdocs/Impl_Plan.pdf

College and University Risk Management Programs

University of Washington Financial Management. (2016) *Risk Management.* University of Washington. Available online at: http://f2.washington.edu/fm/fmat/risk-management

Texas A & M University Risk and Compliance (2016) *Risk Assessment Tools.* Texas A & M University. Available online at: http://urc.tamu.edu/enterprise-risk-management/risk-assessment-tools/

The Ohio State University Risk Management and Insurance (2016) *Welcome to Enterprise Risk management.* The Ohio State University. Available online at: http://u.osu.edu/treasurer/risk/

University of California Office of the President (2016) *Enterprise Risk Management.* University of California. Available online at: http://www.ucop.edu/enterprise-risk-management/

16

Emergency Preparedness Resources

Readiness and Emergency Management for Schools (REMS) Technical Assistance (TA) Center. (2013) *Guide for Developing High-Quality Emergency Operations Plans for Institutions of Higher Education*. U.S. Department of Education. Copy available online at: http://rems.ed.gov/docs/REMS_IHE_Guide_508.pdf

Federal Emergency Management Agency. (2003) *Building a Disaster-Resistant University.* Federal Emergency Management Agency. Copy available online at: https://www.fema.gov/media-library-data/20130726-1457-20490-1338/dru_report.pdf

NYC Emergency Management. (2014) *New York City Hazard Mitigation Plan.* The City of New York. Copy available online at: http://www1.nyc.gov/assets/em/downloads/pdf/hazard_mitigation/plan_update_2014/final_nyc_hmp.pdf

NYC Emergency Management. (2016) NYC Hazard Mitigation Plan Annex. The City of New York. Copy available online at: http://www1.nyc.gov/assets/em/downloads/pdf/hazard_mitigation/2016_hazard_mitigation_annex.pdf

NYC Emergency Management. (2014) *New York City's Risk Landscape: A Guide to Hazard Mitigation*. The City of New York. Copy available online at: http://www1.nyc.gov/assets/em/downloads/pdf/hazard_mitigation/nycs_risk_landscape_a_guide_to_hazard_mitigation_final.pdf