Developing a Comprehensive Risk Management Approach

CAPLAW 2010 National Training Conference

June 16, 2010
3:30 p.m. – 5:00 p.m.

Savannah, GA

Timothy Phillips, Esq.
Senior Corporation Counsel
American Cancer Society, Inc.
250 Williams Street, Ste 4B
Atlanta, GA 30303
P: (404) 929-6842
timothy.phillips@cancer.org

Handouts:

1. PowerPoint Slides
2. Risk Management Process Chart
3. Sample Risk Management Policy

CAPLAW 2010 National Training Conference
Developing a Comprehensive Approach to Risk Management

Timothy Phillips
Senior Counsel
American Cancer Society, Inc.

What is Risk?

- Webster's :

1. the possibility of loss or injury: **PERIL**
2. a dangerous element or factor

What is Management?

- Webster's:

1. the act or art of handling or directing with a degree of skill.
2. the act or art of treating with care.

So….
What is Risk Management?

- Phillips:

1. the act or art of handling or directing with a degree of skill the possibility of loss or injury.
2. the act or art of treating with care a dangerous element or factor.

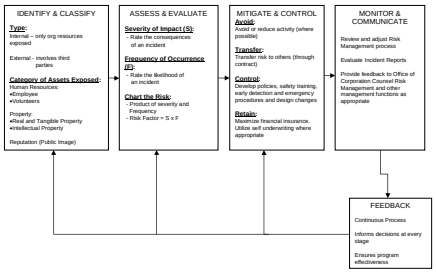
RISK MANAGEMENT MODEL:
Enterprise Risk Management

- Organization – Wide Approach
- Activity Based
- Process Oriented
- Categorize Risks by Effect on Resources

OBJECTIVES

- Provide a framework to manage risks
- Promote risk awareness within the organization
- Identify risks and implement action plans for mitigation

RISK MANAGEMENT PROCESS



RISK MANAGEMENT PROCESS: STEPS

1. Identify and Classify
2. Assess and Evaluate
3. Mitigate and Control
4. Monitor and Communicate

STEP 1: IDENTIFY & CLASSIFY

Risk Areas

- Compliance
- Operations
- Finance
- Reputation/Brand
- Strategic (Mission)

STEP 1: IDENTIFY & CLASSIFY

- Review all activities
- Identify potential liability, loss, damage, or injury that can occur
- Identify potential consequences or negative effect on Society resources
- Classify the risk as Property, Human Resource, or Reputation
- Document control procedure
- Identify Division / Dept. that directs the activity

STEP 1: IDENTIFY & CLASSIFY

Risk Categories

- **Human Resources**
  - Personal Injury to staff, volunteers, or service recipients
  - Criminal Behavior
  - Human Resources Policy violations
  - Communications, information, or technology
- **Property**
  - Theft, damage, or destruction
  - Inappropriate use
  - Income/Revenue Stream
  - Seizure claims by creditors
  - Real and Intangible property (Intellectual Property)
  - Communications, information, or technology
- **Reputation**
  - News Media coverage
  - Catastrophic losses
  - High visibility events

STEP 1: IDENTIFY & CLASSIFY

Sample Risk Register

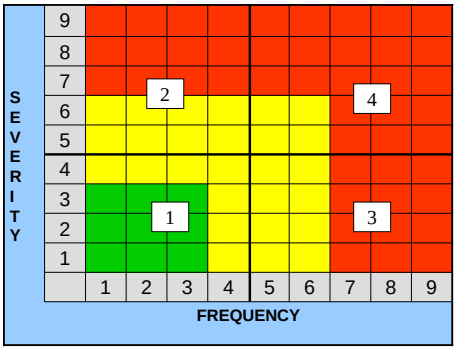
Ref No.	The risk: What can happen and how it can happen	Risk Area	Risk Category (HR, Property, Reputation)	Severity Rating (1-9)	Frequency Rating (1-9)	Level of Risk (L, M, H)	Risk Priority

STEP 2: ASSESS & EVALUATE

- Assess Frequency of occurrence & assign rating
- Assess Severity of occurrence & assign rating
- Calculate Risk Level & priority based on colors on Risk Assessment Matrix
- Evaluate the effectiveness of control procedures and assign rating

STEP 2: ASSESS & EVALUATE

Risk Assessment Matrix



STEP 2: ASSESS & EVALUATE

Risk Assessment Matrix

Steps to using Matrix:

1. Consider what can happen and how it can happen
2. Determine how bad the outcome would be using a scale of Severity (ex. 1-9)
3. Determine how likely it is to happen using a scale of Frequency (ex. 1-9)
4. Chart and calculate the risk level and priority based on the Risk Assessment Matrix

STEP 3: MITIGATE & CONTROL

- Prioritize the highest risks
- Determine to retain or avoid risk (risk tolerance)
- Determine preferred treatment options
- Implement controls to minimize risks retained
- Justify cost of controls vs. potential benefit

STEP 4: MONITOR & COMMUNICATE

- Determine control implementation milestones, timeliness, and targets
- Identify owner responsibility for implementation
- Determine what to monitor and appropriate frequency
- Establish open feedback between owner and legal/risk management department
- Facilitate reporting to Management and Board on program effectiveness

SAMPLE (ACS) RISK MANAGEMENT EXERCISE

Five Identified Areas of Risk

- Disclosure of Personal Information (i.e. private health, credit card)
  - Operations, Compliance, & Reputation
- Advocacy Activities
  - Compliance, Operations, Finance, & Strategic
- Expense Ratio
  - Reputation, Operations, & Finance
- American Cancer Society Brand Abuse
  - Operations, Reputation, & Strategic
- Excess Benefit Transactions (i.e. unreasonable compensation and transactions with Board members)
  - Compliance, Reputation, & Finance

SAMPLE (ACS)
RISK MANAGEMENT EXERCISE

Information Disclosure **Mitigation and Control**

- IT/Data base Audit

Advocacy Activities

- ACS CAN 501(c)(4) (strengthen financial viability)

Expense Ratios

- Functional Allocation Workgroup
- Scorecards and Metrics

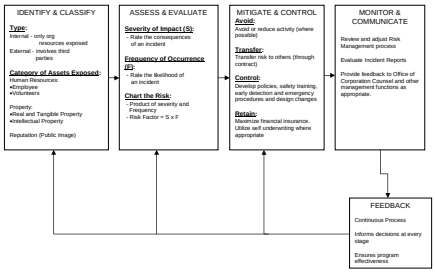
Brand Abuse

- New Licensing Agreement with Divisions
- Active Searches
- Permission Requests

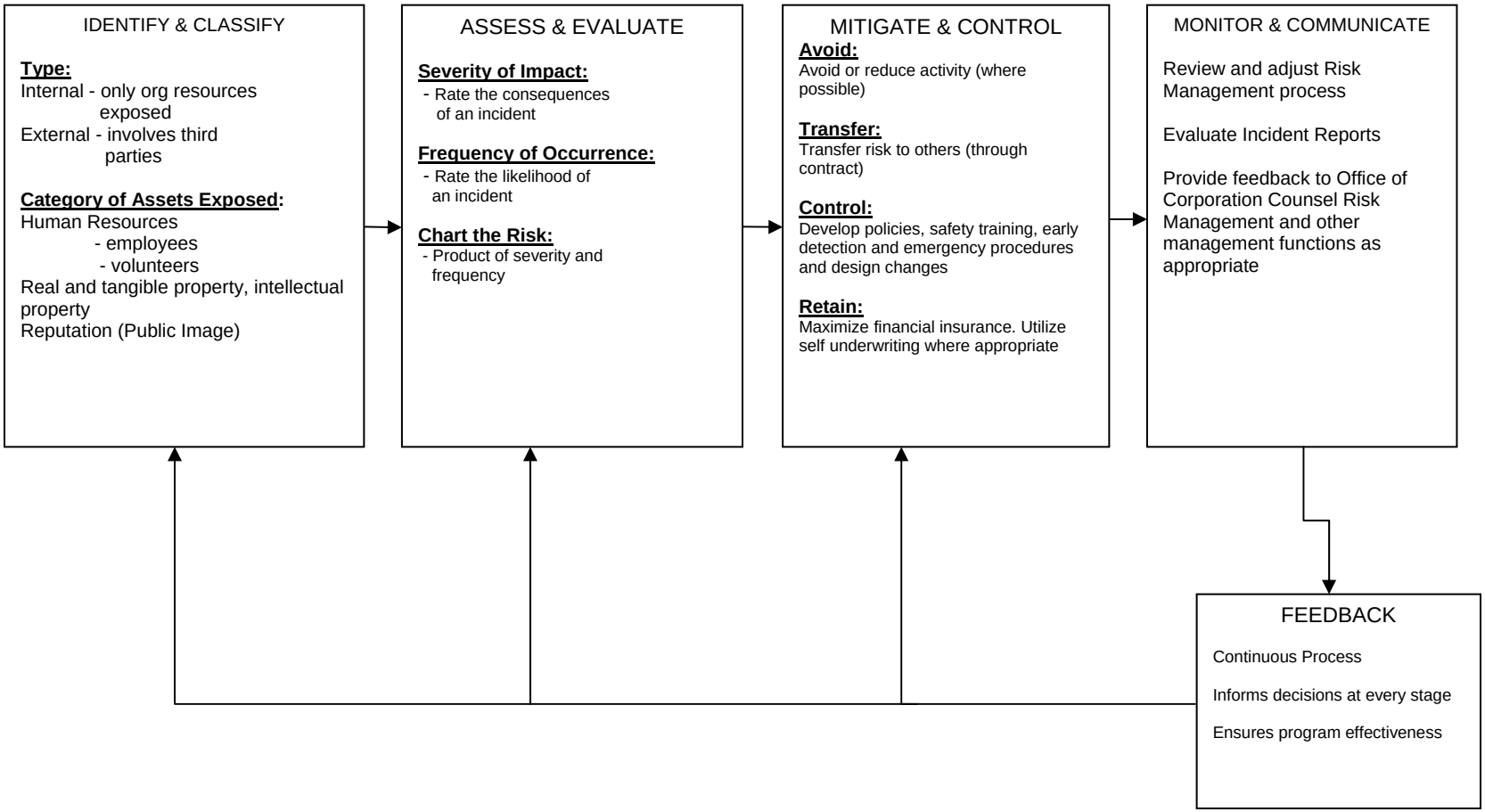
Excess Benefit Transactions

- Executive Compensation Consultant
- Office of Corporation Counsel Audit of Compensation Practices
- Conflict of Interest Workgroup

RISK MANAGEMENT PROCESS



RISK MANAGEMENT PROCESS CHART



[please print in color]

DISCLAIMER:
This is a sample risk management policy. Participants should not simply adopt the policy as their own but rather review it thoughtfully and modify it as necessary to meet the individual needs of their organization and to comply with any applicable state law requirements and grant terms and conditions. Each CAA should consult with an attorney from their state that is well versed in the laws affecting CAAs when working with this policy.

Risk Management Policy

Table of Contents

Introduction

The American Cancer Society ("the Society") is unique in its ability to combine the elements of science, technology and human creativity in the fight against cancer. In its drive to defeat cancer, however, the Society necessarily exposes its human resources, property and reputation to various risks. The Society recognizes the need to actively manage such risks to help prevent losses, minimize liability and prevent unnecessary expenditures.

The policy governs the Society's Comprehensive Risk Management program – a program designed to maximize mission opportunities and minimize financial and operational adversity. Because all manner of risks are present throughout the Society's operations, successful delivery of any of our programs is contingent upon effective and cohesive management of the risks associated with the programs. Risk management is extremely cost-effective when the Society assesses its risks properly and determines the most economical way to limit potential expenditures arising from accidents or emergencies. The risk management process requires:

- An active approach to management;
- Balancing the costs of managing risk with anticipated benefits; and
- Contingency planning in the event that mission critical threats are realized.

1 Comprehensive Risk Management Program

1.1 Program Objective

The objective of the risk management program is to safeguard the Society's property, interests, and the interests of the Society's employees and volunteers during the conduct of activities in furtherance of the Society's mission.

The risk management program ensures the continuity of the Society's operations and services to our stakeholders and promotes stewardship of our donor funds. The Society acknowledges that the adoption of a formal, approach to risk management will improve decision-making, enhance mission delivery and increase accountability. Moreover, the adoption of a risk management policy is consistent with the Executive Limitations on Asset Protection and Reputation contained within the Strategic Governance Policies adopted by the National Board of Directors.

1.2 Risk Management Standards

It shall be the policy of the American Cancer Society to:

Apply the principles of risk management at every management level for the purpose of:

- identifying and evaluating the risks to its human resources, property, brand image and reputation;

- implementing safety and loss prevention measures to minimize exposures to risk;

- avoiding or eliminating risks where practical;

- controlling or contractually transferring risks to others where possible; and

- monitoring and communicating information regarding risk management to employees, volunteers, and third parties.

1.3 Program Application

Consistent with the Charter Agreement between the Society and each Division, this policy applies to all departments and business units that conduct activities on behalf of the Society and its stakeholders. Examples of significant activities include:

Advocacy
Accounting
Business Recovery/Disaster Planning
Brand Asset Management/Reputation Management
Contracting
Ethics and Conflicts Management
Executive Compensation
Facilities Management
Field Operations and Programs (Relay for Life, Road to Recovery, Hope Lodge, Camps, etc.)
Financial Asset Management
Fund-raising and Tax Compliance
Governance
Government Contracts Compliance
Grant-making
Human Resources (Benefits, Labor and Employment)
Information Technology
Insurance/Worker's Comp
Intellectual Property
International Activities
Medical Guidelines (Treatment/Care/Prevention)
Meetings and Travel
Privacy (HIPPA/Research)
Probate Trust Management
Records Management
Security
Transportation
Travel
Volunteerism

1.4 Program Requirements Components

The Society's risk management program is a dynamic process consisting of four interdependent phases: (1) Identification and Classification; (2) Assessment and Evaluation; (3) Mitigation and Control; and (4) Communication and Monitoring. Information communicated in the form of feedback affects decisions made during all phases to ensure that new risks are addressed as they arise and changes to previously identified risks are detected and managed appropriately. A schematic of the comprehensive risk management process is depicted in Appendix A.

1.4.1 Identification and Classification

- The Society shall identify the potential perils, factors and types of risk to which its assets, program activities and interests are exposed.
- Those risks shall be classified into three categories: Human Resources, Property, and Reputation. A detail of each category of risk is outlined in Appendix B.

1.4.2 Assessment and Evaluation

- The Society shall assess identified risks and correlate those risks based on the potential severity of impact (loss, injury, damages) and the likelihood of occurrence (frequency) to determine how they should be managed. A Risk Assessment Matrix is attached as Appendix C.
- Activities should be assigned a residual risk factor (the product of severity and frequency/ divided by the effectiveness of controls) and charted on the basis of this factor. A sample Risk Register is attached as Appendix D.

1.4.3 Mitigation and Control

- The Society shall determine whether to accept, reduce, prevent, transfer or avoid the risk entirely (based on the Society's asset protection limitations, risk/benefit analysis, overall risk appetite) and design and implement cost-effective risk prevention, reduction or avoidance control measures to help ensure the risk decisions are effectively carried out.
- Such measures will include:
  - internal control measures (i.e., policies, best practices reviews, training, safety briefs, and safety checklists);
  - insurance (casualty and theft);
  - contractual transfer (indemnity and insurances clauses in agreements); and
  - self-underwriting risks to which the Society alone is exposed and over which it generally has control, and providing for and absorbing, through annual budgeting, any cost that may arise from self-underwriting.

1.4.4 Communication and Monitoring

- All departments and business units shall:
  - investigate incidents to determine their causes;
  - assess the extent and value of damages and determine potential legal liability;
  - work with the Office of Corporation Counsel to prepare incident reports;

- establish new or improved measures to help prevent the recurrence of incidents;
- maintain their own risk management data-base as part of the feedback system of information management and communication;
- annually review the risk management process to determine its effectiveness
- communicate relevant information to the Office of Corporation Counsel and Corporate Communications to assist in managing any incidents, claims, public perception or litigation.

- The Internal Audit Service function of the Office of Corporation Counsel shall perform periodic audits to monitor and assess the efficiency and effectiveness of the Society's risk management program.

2 Responsibilities

Every staff member of the Society is responsible for the effective management of risk, including the identification of potential risks. Management is responsible for the development of risk mitigation plans and the implementation of risk mitigation strategies.

2.1 Chief Executive Officer

The Chief Executive Officer is responsible for ensuring that a risk management program is established, implemented and maintained in accordance with this policy.

2.2 Finance Committee

The Finance Committee of the National Board of Directors is charged with the oversight and protection of the Society's assets and the identification and assessment of the risks to which the Society's assets are exposed. The Finance Committee shall conduct periodic reviews of the Society's risk management program and may, from time to time, direct that Management provide such reports as will enable the Finance Committee to evaluate the effectiveness of the program and advise the Board accordingly.

2.3 Office of Corporation Counsel

The Office of Corporation Counsel ("OCC") provides legal advice, opinions and negotiation services and is responsible for all litigation concerning claims by or against the Society and against its agents. The Insurance Risk Management function of the OCC provides assistance in risk management training, counseling, program development, and is responsible for monitoring the total cost of risk management. In addition, the Internal Audit Services function of the OCC is responsible for providing Management with analyses, appraisals, recommendations, opinions of internal control, consulting and information concerning the adequacy and effectiveness of the Society's risk management program.

2.4 Corporate Communications

The NHO Corporate Communications Department provides enterprise-wide brand asset management services, reputation management services and internal/external crisis

communications management capacity including surveillance, risk assessment and positioning counsel.

3 Monitoring

3.1 General

Risk management extends beyond merely setting out systems and procedures. The process requires monitoring and assessment. The Director, Internal Audit Services, is charged with the evaluation and improvement of the risk management process utilized by the Society in executing its operational objectives. While IAS is not responsible for the implementation of control measures, it does monitor and review the risk management program and provide periodic reports to both Management and the Board on the effectiveness of the risk management program. To assist IAS in its function and to ensure that the risk management program is a dynamic process, communication with staff at all levels and, where appropriate, volunteers, is critical. Methods of communicating the risks to which the Society is exposed and the measures in place to mitigate and control such risks include the Risk Register and the Risk Treatment Schedule and Action Plan (Appendices D and E, respectively).

3.2 Incident Reports

After the occurrence of a damaging incident, it is critical that any staff members or volunteers involved work with the Office of Corporation Counsel to prepare a timely report that includes the results of an investigation and an assessment of the loss or damages.

Investigating the facts of a harmful or damaging incident has four purposes:

(a) establishing its cause;

(b) assessing the extent and value of damages and potential legal liability;

(c) providing a data-base in support of submissions for approval to pay claims; and

(d) providing feedback on the effectiveness of existing control measures, and acting as a basis for establishing new or improved measures to prevent a recurrence.

Statements in the report should be restricted to the relevant facts and be as objective as possible. Items in the report could include:

- a description of the incident, containing the nature of, and reasons for, the involvement of employees or agents of the Society;

- estimates and an explanation of damages;

- whether any authorities were requested to assist in the investigation;

- whether there was any media involvement;

- the number and dollar value of any claims made and received and whether any further payments are anticipated from the incident;

- whether the incident is in relation to a contract and whether it is consistent with, or deviates from, normal commercial or contractual practices and;

- a summary of the procedures the department has in place to manage the risk of such incidents, as well as the department's approach to any corrective action required to minimize further incidents in the future.

3.3 Internal Monitoring and Direct Inspection Reports

To ensure timely and consistent communication with the Board of Directors, the OCC shall prepare periodic Internal Monitoring and Direct Inspection Reports consistent the Executive Limitations on Asset Protection set forth in the Strategic Governance Policies adopted by the Board of Directors. Such reports will include, but shall not be limited to the following areas of risk management:

- the repair and/or replacement of lost or damaged assets;

- the provision of crime and fidelity insurance policies;

- the protection of the Society's intellectual property;

- internal controls on the receipt, processing and disbursement of funds; and

- internal controls on the purchases of goods, products and services.

4 Measuring Compliance

The Office of Corporation Counsel will inspect and review audit reports prepared by IAS. OCC will conduct an internal investigation of any department or program that demonstrates a failure to implement control measures. Using the results of such investigations, OCC will assist the department or program in instituting the appropriate internal controls. In the event of repeated failures, OCC will recommend review by the Office of the Chief Operating Officer.

5 Inquiries

All inquiries about this policy should be directed to the official designated by each department as responsible for risk management and, when appropriate, to the Office of Corporation Counsel.

APPENDICES

A. Risk Management Process

B. Developing the Universe of Risks

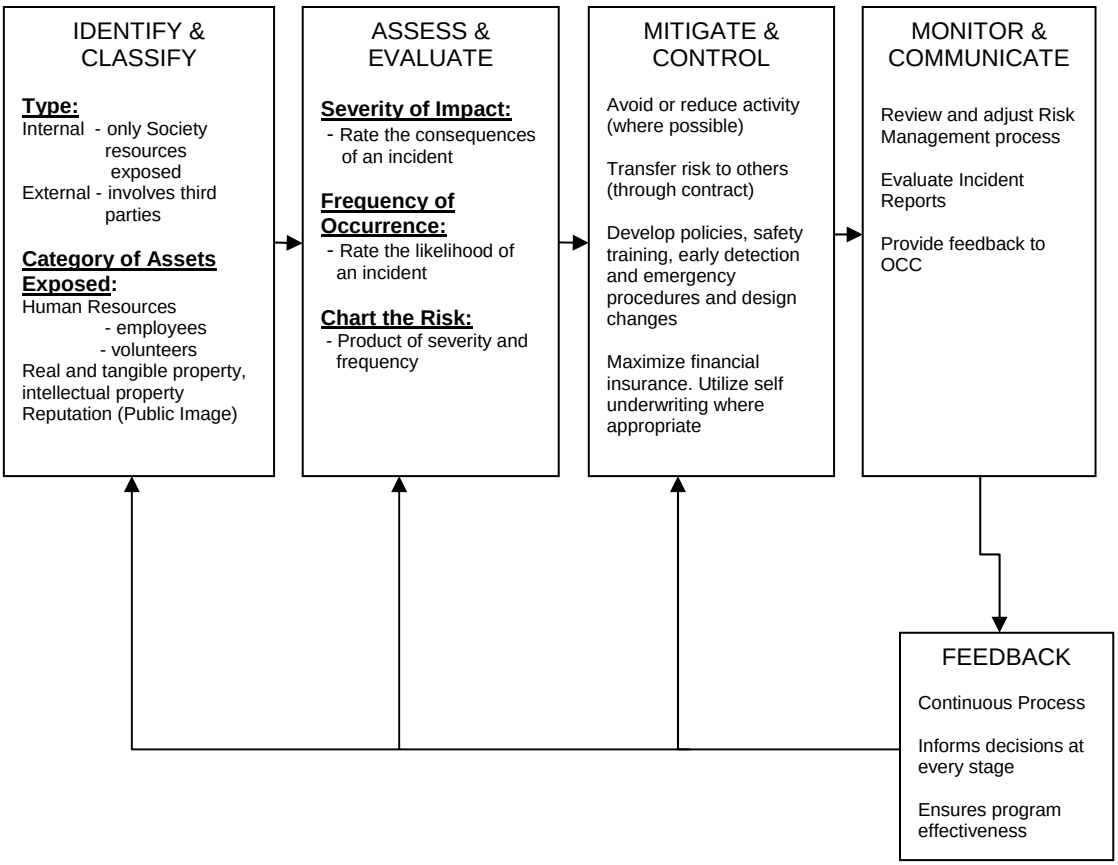
C. Risk Assessment Matrix

D. Sample Risk Register

E. Sample Risk Treatment Schedule and Action Plan

Appendix A - Risk Management Process

RISK MANAGEMENT



Appendix B – Developing the Universe of Risks

Step 1
Identify the ACS Program or Activity, e.g. Relay For Life, International Conferences, Cause Related Marketing

Step 2
Identify which risk areas are present

Operational
– Does the activity expose ACS resources or assets to risks of loss or damage?

Legal
– Is the activity regulated by federal state and local law?
– Does the activity expose ACS to claims by participants, creditors or service recipients?

Reputational
– Can the activity negatively impact ACS public image or perception?

Step 3
Classify risks in one of three categories

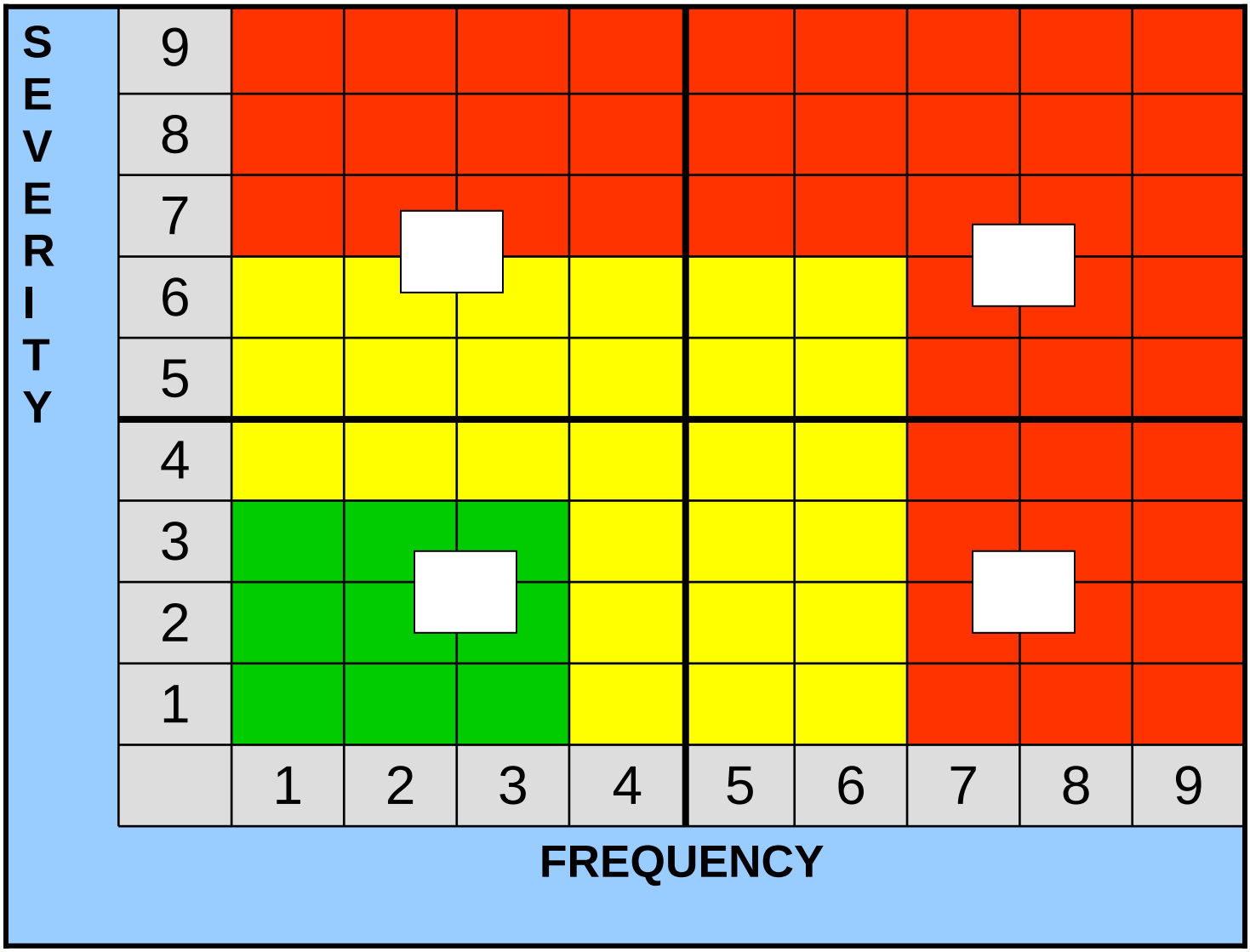
Risks to Human Resources
Risks to Property
Risks to Reputation

Risks to Human Resources
- Personal Injury to staff, volunteers or service recipients
- Criminal behavior
- Human Resources violations
- Communications, information, technology

Risks to Property
- Theft , damage or destruction
- Inappropriate use
- Loss or abandonment
- Seizure claims by creditors

Risks to Reputation
- Media communications
- Catastrophic losses
- High visibility events

Appendix C – Risk Assessment Matrix



Risk Likelihood/Frequency Ratings, Risk Consequence/Severity Ratings, Effectiveness of Controls

Risk Likelihood Ratings	
Likelihood	**Description**
Almost Never / Rare [1-2]	The risk event may occur only in exceptional circumstances, eg. up to 4% chance of occurring in the next 12 months (or once in 25 years).
Unlikely [2-3]	The risk event could occur at some time, eg. 10% chance of occurring in the next 12 months or 1 out of every 10 years.
Possible [3-5]	The risk event should occur at some time, eg. 25% chance of occurring in the next 12 months or 5 out of every 20 years.
Likely [6-7]	The risk event will probably occur in most circumstances, eg. 55% chance of occurring in the next 12 months or 11 out of every 20 years.
Almost Certain [8-9]	The risk event is expected to occur in most circumstances.

Risk Consequences/Severity Ratings	
Risk Consequence/Impact	Definitions
Minor [1-3]	- financial impact of up to $25,000 in any 12 month period; and/or - loss or reputation or image that involves local adverse media coverage; and/or - event that involves management time.
Moderate [3-5]	- financial impact on of up to $100,000 in any 12 month period; and/or - loss of reputation or image that involves widespread, adverse media coverage and/or potentially involves litigation; and or - event that involves a reasonable amount of management time.
Severe [5-7]	- financial impact of up to $500,000 in any 12 month period; and/or - loss of reputation or image that may take up to 1 year to recover and/or potentially involve litigation; and/or - event that involves significant management and/or Corporate Counsel time.
Major [7-8]	- financial impact of up to $1 million in any 12 month period; and/or - loss of life or serious harm injury; and/or - event that prevents ACS implementing all or part of its strategic plan and involves significant Board time; and/or - loss of reputation or image that may take 1-3 years to recover and involves a damaging litigation claim.
Catastrophic [9]	- financial loss of $1 million or more in any 12 month period; and /or - multiple loss of life; and/or - loss of reputation or image that may take 3-5 years to recover.

Effectiveness of Controls	
Very poor [1]	20% or less, effective
Unsatisfactory [2]	30% approximately effective
Good [3]	50% approximately effective
Very Good [4]	70% approximately effective
Excellent [5]	80% plus, effective

Appendix D – Sample Risk Register

Date of risk review_____

Compiled by: _____ Date: _____

Reviewed by: _____ Date: _____

Function/activity _____

Ref No.	The risk: What can happen and how it can happen	Risk Area	Risk Category (HR, Property, Reputation)	Severity Rating (1-9)	Frequency Rating (1-9)	Level of risk (L, M, H)	Risk Priority

Appendix E – Sample Risk Treatment Schedule and Action Plan

Date of risk review_____

Compiled by: _____ Date: _____

Reviewed by: _____ Date: _____

Function/activity _____

The risk in priority order from Risk Register	Possible treatment options	Preferred options	Risk rating after treatment	Result of cost/benefit analysis A: accept B: reject	Person responsible for implementation of option	Timetable for implementation	How will this risk and the treatment options be monitored

RISK ACTION PLAN

Item	Ref
Risk	
Summary – Recommended Response and Impact	
Action Plan 1. Proposed actions 2. Resource Requirements 3. Responsibilities 4. Timing	