Washington State Department of
Enterprise Services

RISK MANAGEMENT BASICS

OFFICE OF RISK MANAGEMENT

AUGUST 2017

Table of Contents

Introduction

"Risk Management Basics" is an overview of information keyed to new risk managers in Washington state agencies. It is written in short, stand-alone segments that can be used as an overview or introduction to risk management subjects. In each segment, links or contacts for related resources are provided.

For more information or training ideas contact:

Jean Jelinek, Loss Prevention Coordinator

360.407.8158

Jean.Jelinek@des.wa.gov

What is Risk?

What is Risk?   "Risk" is defined as anything—good or bad, big or small—that could prevent the achievement of a goal. Risk is a natural part of life and though we can list, measure and mitigate it, we can never completely eliminate risk.

We deal with risk every day in our private lives. Groups of people, however, need a formal process to deal with the risks they face, and the term "risk management" is used to refer to the various practices an organization uses to manage risks.

In government, the level and types of risk vary among agencies, as well as within agency divisions. Regardless of the agency's mission, each agency faces risks. These risks must be identified and managed to protect the state's employees, resources, citizens and reputation.

Find Out More   Enterprise Risk Management

Risk Management Today

Risk Management Today

Risk has always been with us, but the demands on and concerns of today's risk manager are very different than they were 20 years ago. Back then, risk management was centered on concerns such as fire drills, bad weather and whether clients might slip and fall in the lobby. Today, this is often referred to as traditional risk management.

Risk managers usually have experience with traditional risk areas and have years of data available for making decisions. Traditional risk areas, which are generally associated with some type of insurance product, include:

- Worker safety
- Auto liability
- Property
- General liability
- Compliance (sometimes called regulatory liability)

Modern risk managers still handle traditional risk issues. In addition, they must master the skills needed to face an increasing number of new, non-traditional challenges from inside and outside the agency.

These new demands have forced the practice of risk management to look for a more cohesive and comprehensive structure. This structure is referred to as Enterprise Risk Management (ERM). Enterprise risk management brings value to agencies by using a strategic approach to risk management that is more responsive to the new risk environment.

New Skills and Opportunities

Risk managers have begun to develop methods to assess and measure the new generation of risks never before quantified. This required them to use techniques other than math or econometric-based systems. It also has made it possible for risk managers to talk about risk more clearly.

With ERM methods, risk managers can work across the agency to identify, measure and evaluate any kind of risk. With ERM, leaders can, for the first time, get a clear "big picture" of their most serious exposures and make informed decisions about how to deploy resources to lessen risks that threaten successes.

More than ever before, skilled risk managers are playing a prominent role in the strategic efforts of their agencies and becoming part of a major wave of change in how risk is viewed and managed.

Risk Manager Competencies

Risk Manager Competencies

The well-rounded risk manager needs skills and experience in many areas. In addition to analytical, change management and policy-making skills, you will likely need to be an expert facilitator, communicator and maybe a mediator.

Because new risk areas are constantly emerging, no risk manager can afford to stop learning. Depending on your agency, you may be, or need to become, an expert in some risk management areas while having a general understanding of other topics (but know where and how to get more information when needed). At the least, risk managers should know the basics in each of the following risk management areas:

- The risk management process
  - Traditional risk management model (1. Identify hazards; 2. Assess and prioritize risks; 3. Choose control measures; 4. Implement controls; and 5. Monitor and review results)
  - Enterprise risk management model (1. State goal; 2. Identify risks; 3. Evaluate risks; 4. Prioritize risks; 5. Treat risks; 6. Monitor and review results; and 7. Communicate results)
- Loss prevention
  - Incident reporting
  - Root cause analysis
- Insurance
  - Self insurance and commercial insurance
  - Uses of and need for reinsurance
  - Certificates of insurance
  - Contractor and lease indemnification and insurance
- Claims management
  - Tort claims
  - Litigation
  - Workers compensation
  - Return to work
  - Loss history
- Health and safety
  - Driver safety
  - Worker safety
  - Emergency management
- Records management
  - Confidentiality
  - Data security and cyber liability
  - Information technology
  - Privacy violations

- Public disclosure
- Records retention
- Regulatory compliance
  - State and federal program and employment regulations
  - Financial regulations
  - Internal control

Risk Management Partners

Risk Management Partners

The work of risk managers puts them in contact with many people who work with their agency, from executive staff to contractors. Developing internal relationships helps in all parts of the risk management process.

It is also helpful to reach out to the risk management community around you. You will find valuable colleagues in other parts of your agency, in other state, county and city agencies, and in the national and international risk management community, including those who are:

- Safety managers: Risk management and safety management are closely aligned and share many of the same issues and goals.
- Internal auditors: Agency internal auditors are experts in measuring how well an agency controls its risks. They can be valuable partners in measuring the success of new risk management processes.
- Facility managers: Facility managers are often the first to find out when an incident occurs and may be the first to respond in a crisis or emergency.
- Human resource (HR) managers: HR personnel must be involved in agency efforts to meet employment, return-to-work and retention goals.
- Emergency Management: Risk managers are often closely involved with the development of plans, training and drills to respond to natural disasters and other emergencies.
- DES-Office of Risk Management: DES provides consultation, education, training and support in all areas of risk management, as well as regular opportunities to network with risk management colleagues.
- Others: Public records officers, records retention officers and security officers are important risk management partners in the protection and safeguarding of confidential information. They can assist you in developing the actions required to prepare for and respond to an information breach.
- RIMS (Risk and Insurance Management Society): RIMS has private and public sector members worldwide, hosts regional and national conferences and has a Washington chapter. It provides education and daily updates on risk management news on its website.
- PRIMA (Public Risk Management Association): PRIMA is a national organization targeted to public sector risk managers. It sponsors a Washington chapter and offers regional and national annual conferences. PRIMA also provides education, news and updates on its website.
- PERI (Public Entity Risk Institute): PERI is a nonprofit research institute that develops risk management education and training

resources for local governments, school districts, small businesses, nonprofits and others.

- IRMI (International Risk Management, Inc.): IRMI's mission is to be the premier authority in providing expert advice and practical strategies for risk management, insurance and legal professionals.

- STRIMA (State Risk and Insurance Management Association): STRIMA works with other state government risk management offices, Canadian provinces and insurance professionals to promote the advancement of risk management principles and practices in state and provincial government.

Find Out More
- DES Risk Management
- RIMS
- PRIMA
- STRIMA

When Things Go Wrong

When Things Go Wrong

Even in the best-run agencies, things go wrong. When they do, people turn to the risk manager for help. So risk managers routinely set up systems—usually in partnership with safety managers, facilities managers, human resource managers, internal auditors and others—to help staff respond when an emergency, injury, lawsuit or other unexpected event happens. Every employee should know what to do when things go wrong.

What to do Immediately

Teach employees that, when something bad happens, the first and most important thing to do is respond as soon as possible, and:

- Be sympathetic without placing or accepting blame. (See RCW 5.66.010.) Call emergency workers, if needed. Stay with the person, or at the scene, until help arrives.
- Report what happened to the next available person in the chain of command. Follow agency policy about further reporting.
- Review the event later to learn how the same thing might be prevented or better responded to in the future. (See "Root Cause Analysis.") If appropriate, contact the person or people involved to see if additional help is needed.

If a Worker is Injured

The Department of Labor and Industries' (L&I) website (www.lni.wa.gov) provides information on when and how an injured employee files a claim and what paperwork to expect.

Not all workers understand they have to immediately report work-related injuries and illnesses to their employer and to L&I, or that the employer is also required to respond to the report of injury to L&I in certain circumstances. (See Chapter 51.28 RCW.) Make sure that employees are aware of and follow internal policies for reporting injuries.

When a Client is Involved

Before an injury happens, decide what the agency is able to do to help if a client/customer or citizen becomes injured. Let employees know that it is ok to say to an injured client something like, "I am sorry this happened to you" and "How may I help?" Train employees to file an incident report immediately after they respond. Work with appropriate staff to review the incident later to look for patterns, trends or changes needed.

Tort Claims and Lawsuits

Sometimes people who feel the state is responsible for their loss (including state employees with employment complaints) will say they are going to sue or want payment for their loss. Let agency staff know that it is ok to give the person information about filing a tort claim,

including providing a copy of the tort claim form. (See "Tort Claims" or the DES Risk Management website for more information at [Standard Tort Claim](#).)

Damage to the Facility   Due to bad weather, fire, building failure or a threat, buildings sometimes have to be closed or evacuated. In these cases, call police, fire or other emergency workers first if they are needed. Have a plan already in place to notify everyone, including the public, when agency buildings have to be shut down. Communication is critical—make sure everyone knows the plan and can respond quickly in an emergency. Consider posting emergency plans on your agency Web site.

If you are in a leased facility, know the landlord's responsibility to respond if the damage is caused by a building failure like a roof leak or a heating/ cooling problem, or if the problem is an emergency such as a fire or earthquake. Post information on how to contact landlords and emergency services in several locations throughout the facility.

Take a Picture   Photos of damage or events can be useful later. Whether it's a fender-bender in the parking lot, injured employee or flooded building, encourage employees to take a picture whenever possible. If someone reports damage at another location, try to get a picture for the agency's incident file from someone on site. Include a description of where the picture was taken, who took it and the date taken.

Incidents and Incident Reporting

Incidents and Incident Reporting

Risk managers generally use the term "incident" to describe a sudden, un-expected (generally negative) event that is outside the norm of what happens at work. The term used and the exact definition of an "incident" may vary by agency.

Incident Reporting

Whatever they are called, it is important for employees to report incidents and for risk managers to keep track of them. Incidents that aren't reported cannot be managed, and incidents that aren't managed can create multiple unwanted outcomes, including claims and litigation.

Small incidents and "near misses" may not seem to make a difference to a large agency, but encouraging people to report these events has benefits. This reporting:

- Shows that the agency cares about what happens to individuals.
- Provides an "early warning system" for events that might later develop into workers compensation claims, tort claims, lawsuits, discrimination complaints or other employment actions, or media events.
- Helps risk managers spot trends, identify areas of concern and plan training or other mitigation strategies that address priority risks to the agency based on real information, not anecdotes or guesswork.

Some incidents will also need to be reported to designated agency leaders or to the Governor's Office, DES Risk Management, State Auditor's Office or another agency. Each agency should have a clear policy about incident reporting and how to follow up with investigations of report incidents, when necessary.

Responding to Incidents

Each risk management program should include clear, easy-to-use instructions on how people can respond to incidents. Whether the agency's incident response policy requires each employee to respond directly, requires the risk manager to be involved with incident responding, or requires an incident review team to be assembled, the process should allow the agency to quickly solve as many problems arising from an incident as possible. A fast response to an incident generally limits the damage and may lessen the likelihood of litigation.

The Loss Prevention Review Team Program and Reportable Incidents

Incident Reporting

The Legislature has directed state agencies to report the following types of incidents to DES. (See RCW 43.19.782)

1. Death of a person
2. Serious bodily injury to a person
3. Substantial loss

More information about reporting is posted on the DES website at Incident Reporting.

Loss Prevention Review Team

Pursuant to RCW 43.19.782, all state agencies are to appoint a loss prevention review team when the death of a person, serious injury to a person, or other substantial loss is alleged or suspected to be caused at least in part by the actions of a state agency *except* when the death, injury or substantial loss is already being investigated by another federal or state agency.

The Department of Enterprise Services may also direct a state agency to a conduct a loss prevention review and, if requested, may provide guidance to a state agency conducting a loss prevention review.

The Review Team:

1. Consists of a least three persons and may include independent consultants, contractors, or state employees.
2. Cannot include any person directly involved in the loss or risk of loss giving rise to the review, nor any person with testimonial knowledge of the incident to be reviewed.
3. At least one member of the Review Team will have specific expertise in the topic of the review.
4. No more than half of the members may be employees of the affected agency.

An LPRT may include independent consultants or contractors. State employees and agency personnel knowledgeable about the incident may be asked to provide information or meet with the LPRT.

When the review is complete, the LPRT provides a written report to the affected agency and the DES director. The report is posted on the DES Web site at LPRT Reports.

Find Out More

- LPRT Program Requirements
- Incident Report Form

Root Cause

Root Cause Analysis

Root Cause Analysis (RCA) is a systematic process for identifying the underlying cause of a problem or event and finding a way to avoid or reduce the severity of such problems or events. The process is used in a variety of settings.

In all RCA methods, remember that the focus of investigation and analysis is *why* the event occurred, not *who* made the error. Whatever method is used, the key steps are the same:

- State the problem
- Gather information, data and evidence, as needed
- Determine the root cause of the problem
- Identify recommendations to prevent a recurrence
- Implement the solution

When to Use RCA

RCA is a rigorous process that involves many people and may result in recommendations for change. In the risk management setting, reserve RCA investigations for high-risk, high-impact events where the cause is not understood and the need to prevent recurrence is high. RCA is not often used for events involving criminal acts or requiring disciplinary action because these events are investigated by law enforcement and/or HR personnel.

Because the RCA process relies on information from people involved in the event, it should be started as soon as practicable. The passage of time can dim accurate accounts of events, leading to less reliable information.

Near Misses or Close Calls

If you notice a pattern of "near misses" or "close calls" for high-impact events, consider an RCA, which may help prevent additional incidents.

Confidentiality

If any information to be reviewed is confidential under state or federal law, the RCA planning process should include provisions to ensure confidentiality. In these instances, RCA team participants should sign a confidentiality agreement before the process begins.

Guidelines

Whatever method is used, RCA must take place in a blame-free environment. It is designed to find and correct circumstances or failures in *systems*—not *people.*

Statements of root causes of events should show the cause and effect relationship between the root cause and the harm. Statements should not be negative or inflammatory. Don't say that "Some idiot left the

cheese out for the mice to eat." Do say that "The cheese was on the kitchen counter for three hours when staff were not in the area. Mice ate the cheese."

If the cause is an action, state the condition(s) that caused the action. For example, in a case where a patient dies on the operating table, the direct cause might be that the nurse didn't recognize the symptoms leading to the death. The condition that caused the death could be that the nurse was new, and the specialized training needed to recognize the particular symptoms is not given until a nurse has 30 hours of operating room experience. In this case, the root cause is the timing of the training.

When the cause is a procedural deviation, identify the cause, as well as state what happened. For example, don't say that "The agency was fined $1.5 million for not adhering to federal reporting standards," which is a statement of what happened, not a cause. Do say that "The program did not collect data needed to monitor the grants at specified intervals because the program had not been added to the chart of accounts. The chart of accounts was not amended because the agency does not have a standardized process for receipt and administration of new grant programs." In this case, the root cause is not having a standardized process for adding new grant programs to the chart of accounts.

The "5 Whys"

The "5 Whys" method is a popular and simple RCA problem-solving technique that helps users get to the root of the problem without special software or statistical tools.

The "5 Whys" strategy involves looking at a problem and asking "Why did this happen?" and "What caused this problem?" Although the method is called the "5 Whys," you may need more or less than five questions, depending on the complexity of the event. The idea is to keep asking "why" until the underlying cause is revealed. Here's an example:

Problem Statement:

Ms. X was on the way to a meeting and the agency car she was driving stopped in the middle of the road.

Why did the car stop? *Because it ran out of gas.*

Why did it run out of gas? *Because the last person who used it didn't fill it.*

Why didn't the last person fill the tank? *Because that person didn't know that one of the requirements of using the car was to fill it before returning.*

Why didn't they know? *Because that person is new to the agency and there is no policy or training on car use.*

15

Why is there no policy or training? *Because in the past, all drivers were agency veterans who knew the expectations and no one needed to be familiar with a policy or undergo training.*

The final "why" should lead the team to a statement of the underlying cause. The team can then decide if change is needed to keep agency cars on the road.

Asking the Right Questions

While the "5 Whys" is a simple and quick method, it can lead to a misleading analysis if the wrong questions are asked or the process is stopped before the root cause of a problem is reached. Make sure agency RCA team(s) are properly trained, or use experienced facilitators to keep the process rigorous and focused while it is being learned by staff.

Find Out More

- Root Cause Analysis
- L&I Accident Investigation Basics Online Course

Enterprise Risk Management

ERM Overview Traditional risk management focuses on mitigating losses. The risk manager follows up an event and analyzes loss information to determine if the agency should change its operations or policies to better protect the organization, clients and employees from similar losses in the future.

ERM is a risk management method that begins with goals. ERM looks at important agency goals (not just accidents or lawsuits) and the risks connected to each goal. In this context, a "risk" is anything—good or bad—that could stop you from reaching a goal.

Once a goal is clearly defined, ERM uses a simple process to identify, evaluate and prioritize all the risks to achieving it.

After the most severe risks are identified, a treatment plan is developed for each that matches the organization's level of control, risk appetite and available resources. Successful ERM:

- Includes all parts of the agency.
- Requires open communication from all levels of the agency about goals, operations and potential problems, and fosters clarity of purpose.
- Results in a high-level review of the risks most likely to affect important agency goals.
- Provides an easy-to-use, proven method to evaluate and address risk at all stages, including strategic planning, as well as post-incident review.

ERM Advantages The ERM method provides a wider perspective on risks. It helps an agency identify and address risks beyond the traditional type of risk usually considered, such as worker safety, driver safety, tort liability, etc. ERM helps agencies engage everyone in deciding how to meet goals and where to deploy scarce resources for the best outcome.

ERM is Flexible The ERM process has its roots in England, where it is still part of government practices. It is now used throughout the world in government and business settings. As to be expected with a widespread process, modifications have been adopted that make it responsive to individual organizations. ERM *is* flexible and *should* be adapted to the group using it for best results.

How ERM Defines "Risk" In traditional risk management, risk is defined as a negative outcome such as an injury, car accident, workers compensation claim, safety violation, audit finding, tort claim, lawsuit or other "failure."

ERM defines risk more broadly as anything that could prevent the achievement of a goal. Risk is also commonly understood as: (a) variation, (b) from the objective, (c) over time.

This change in focus affects how risk is evaluated and treated in ERM. It requires an agency to look beyond injury and accident rates to underlying goals and to evaluate anything—good or bad, big or small—that could affect achieving goals.

Successfully assessing and mitigating risk this way requires collaboration. It can't be done by a risk manager working alone at a desk. Only the people who understand how a program or process works can realistically and practically know what factors are likely to affect reaching the goal.

Understanding Risk "Appetite"

The level of risk that a person or agency can tolerate is referred to as "risk appetite" or "risk tolerance." It varies among individuals and groups depending on values, history, type of risk and possible negative outcome under discussion. Some can tolerate little risk while others are comfortable risking everything if the outcome is important enough.

This can lead to conflicts when goals and plans are under consideration. Resolving this conflict is easier when participants understand that their own and others' tolerance for risk may be different.

Determining Influence and Control

"Control" can refer to influence or, more commonly in risk management, to the procedures or processes that an agency puts in place to establish control in risky areas (such as policies, routine audits or separation of duties in parts of an agency where payments are authorized).

When assessing risk, it is important to understand how much control the agency has over a risk because that influences how each risk is evaluated and treated. In most ERM methods, control is evaluated by assigning a "low," "medium" or "high" control rating.

Voting To Select Priorities

After identifying the risks to reaching a goal, each is assessed using a five-point scale to determine how likely the risk is to happen and how seriously the risk would affect reaching the goal. These numbers may be obtained by having participants vote anonymously and averaging the results. This is a reliable way to foster full participation and obtain an accurate group assessment.

Establishing a Blame-Free Environment

The goal of the ERM process is to clarify goals and reduce serious risks to meeting them. ERM is not concerned with looking for people to blame when things go wrong or when goals are not met. Individuals should know their contributions are important and feel free to discuss potential

risks in an open and blame-free environment. ERM works best in an atmosphere where people feel they are working together to achieve something important.

Building Risk Maps

After voting, the scores for identified risks are plotted on a graph that measures likelihood on one axis and impact on the other axis. This map displays how the group has ranked the identified risks and allows the group to decide which risk(s) should have the highest priority for action. Most risk maps use color to show priority, with red in the area where the highest scores fall.

Treating Risk

Once the most important risk(s) are identified, the next task is to develop a plan to mitigate or "treat" the risk(s). In ERM, you can:

- Avoid (usually by discontinuing the activity)
- Accept and monitor (this should include setting a threshold to begin treatment)
- Reduce the likelihood
- Reduce the impact
- Transfer (generally through insurance or a contract)

Follow Through

Identifying risks is important to the ERM process, but the purpose of ERM is to increase the chances of meeting critical goals. Don't stop after the risks are identified. It is important to do the hard work of the treatment plan.

Creating a Risk Register

A risk register is a document that details the risk assessment by providing a list of high-priority risks to reaching the goal and an overview of how each will be handled. It includes:

- A short description of the risk and the final score or voting results
- Which of the five treatment options was chosen
- A brief description of the treatment plan created to reduce/control the risk
- A short description of how to measure the success of the treatment plan
- Important target dates in the plan
- Person responsible for the risk treatment plan (sometimes called the "risk owner")

Sharing Best Practices

At the end of the treatment plan, it is important to reassess the risk, decide how well the plan worked, and determine if monitoring or further action is needed. Treatment plans that work should be shared and the lessons learned communicated as "best practices" to other parts of the agency that could use the techniques to good advantage.

7 Steps to ERM

The 7-Step method is simple, quick and easy to use while incorporating all ERM fundamental principles.

7 Steps Overview

1. State the goal
2. List everything that could keep you from meeting the goal (the risks)
3. Evaluate each risk:
   - Choose a likelihood rating from 1-5
   - Choose an impact rating from 1-5
   - Multiply together and map
4. Prioritize:
   - Use your risk map to identify the most severe risks
   - Decide which risks to concentrate your efforts on (for your designated time period and time, and staff and money resources)
5. Treat/mitigate:
   - Avoid
   - Accept and monitor
   - Transfer
   - Reduce the likelihood
   - Reduce the impact
6. Make a risk register that includes:
   - Treatment plans
   - Measures of success
7. Communicate results:
   - Gather and share best practices
   - Review and refine

Step 1: State the Goal

State your goal in positive terms. People often miss the "not" in a statement and develop the opposite understanding. If your goal is positively stated, it will be easier to talk about the barriers to not achieving it than to list everything that could prevent you from *not* doing something.

Be specific and precise in stating your goal so that everyone understands what is being discussed. Whenever possible, make your goal about operational details that people can discuss. Before you begin to gather risks, make sure participants are satisfied with the goal statement, and if it doesn't work, change it.

Programs, people and conditions change. Set a realistic deadline for how long it should take to accomplish your goal.

Step 2: List everything that could keep you from meeting the goal (the risks)

Whenever possible, include everyone who is involved in meeting the goal when you generate the list of risks. These are the people who know what might go wrong.

List everything, good and bad, big and small. Let everyone participate and write down every risk that is generated. The most unlikely statement may turn out to be the biggest, most realistic risk to meeting your goal.

Speak freely about concerns to improve communication and foster trust in work groups. Remind participants to state thoughts in the form of a risk, not a complaint or opinion. Depending on your goal, you may want to include risks generated by clients or stakeholders as well.

Check your results widely. You may be able to start with a small group, but if others are involved, broaden your collection of risks to include them. You might want to consider a survey approach.

Consider the values of individuals and the group as you generate the list of risks. Sometimes beliefs, culture or the ethics of a profession will generate risks that wouldn't show up elsewhere.

Don't be distracted by "cures" at this point. As the discussion of risks progresses, it is natural for the group to start talking about how to fix each risk, but it is too early in the process to talk about cures. If you find yourself discussing a cure, write down the risk that is being "cured" and then return to listing other risks. The objective for this part of the process is to concentrate on gathering a comprehensive list of risks.

Step 3: Evaluate each risk

RISK MAP		Impact				
		1 Very Little	2 Minor	3 Moderate	4 Major	5 Critical
Likelihood	5 Certain	(5)	(10)	(15)	(20)	(25)
	4 Very Likely	(4)	(8)	(12)	(16)	(20)
	3 Likely	(3)	(6)	(9)	(12)	(15)
	2 Unlikely	(2)	(4)	(6)	(8)	(10)
	1 Very Unlikely	(1)	(2)	(3)	(4)	(5)

Once the list of risks is complete, the group should evaluate each risk by assigning a number from 1 to 5 that shows how likely it is that the risk will happen. Once this is done, evaluate what the impact to the goal would be if it did (also on a 5 point scale). These two numbers should then be multiplied together so that each risk can be plotted on a risk map like the one pictured above. (It is common to see different words used to describe the map, scores and categories, like

"Frequency/Severity" or "Likelihood/Impact." Use words that work best for your group.)

The most realistic results come from voting anonymously. If done as a group, the most influential people in the group may change others' votes (whether through status, decibel or persuasion). If you have access to an Audience Response System to vote with keypads, this is a great way to plot the group evaluation. If not, each person can do a private computation and then all the numbers can be added and averaged for the final score.

Step 4: Prioritize (pick the most severe risks)

Once each risk is evaluated and a group score between 1 and 25 is assessed, plot the risks by score on a risk map. When a color-coded map is used, the most severe risks fall in, or close to, the "red zone." Even if a color-coded risk map is not used, the most severe risks will fall in the top, right quadrant where the highest scores for impact and likelihood meet.

For some goals, a decision might be made to work on several risks at once. Most often, unless the agency has unlimited resources of people, time and money, the group will have to pick one or two of the most severe risks to work on.

Step 5: Treat/mitigate the priority risks

In ERM, there are five ways to treat a risk. For each risk, choose one of the following treatments:

- **Avoid**
  The only way to avoid a risk is to stop the activity. Unlike a business, government agencies may not have the choice to stop providing a service or program. Yet an agency may be able to change *how* a service is delivered to avoid a risk.

- **Accept and monitor**
  This choice requires you to develop measures to track whether the risk gets better or worse over time. If the agency has very low control over a risk (such as national economic conditions or natural disasters), this can be the best treatment choice.

- **Reduce the likelihood**
  Treatment should focus on making it less likely that the risk will happen by reducing the conditions that cause the risk (like ice on a sidewalk) or by reducing the number of occurrences (such as complaint calls that aren't returned).

- **Reduce the impact**
  This option aims to reduce the effect on a goal if a risk happens. If your goal, for example, is to keep all agency confidential information secure, then requiring password encryption of confidential information on all laptops will lessen the impact on the goal if a laptop is lost or

stolen.

- **Transfer**
  Risk can be transferred either through an insurance policy or a contract that requires the contractor to assume the risk that comes with not meeting the goal.

No matter which treatment is chosen to address a risk, the treatment plan will not work unless it:
- Fits the risk appetite of your group
- Reflects the actual amount of control you have over the risk
- Is measurable and time-limited
- Explains what needs to be done, who is responsible and what measure will be used to show whether the plan succeeds

Treatment plans may be elaborate action plans with multiple steps and due dates, or they can be simple, one-line "overview" explanations. Either method can be successful as long as the group understands the plan and accepts the format.

Once the risks are collected and evaluated, priority risks identified and treatment plans developed, pull all the information together in a risk register. A risk register is a list of priority risks with an overview of how each risk will be handled. Some organizations and industries use sophisticated software programs to generate risk registers, but most find that a chart like the one pictured below works for their ERM efforts.

GOAL:				
Risk (Briefly describe; include score)	**Risk treatment (Check type and briefly describe)**	**How will we know when we succeed? (List success measures)**	**Target date**	**Person responsible**
	□ Avoid □ Accept □ Reduce □ Transfer			
	□ Avoid □ Accept □ Reduce □ Transfer			

No matter what format you choose, preparing a risk register has clear advantages. Your agency risk register:

- Serves as a comprehensive and ranked list of critical business issues
- Sets clear priorities for action
- Provides a defensible basis for decision making and funding
- Improves communication and fosters clarity of purpose
- Achieves reconciliation and coordination of competing values
- Demonstrates credibility (the ERM method is a recognized international standard for managing risk)

Step 6:
Follow the plan

A risk assessment process can stall after the excitement of the initial work subsides. When people go back to their desks, they get pulled in other directions and may have trouble starting the planned risk treatments.

A risk manager keeps communication alive by involving other people in the risk assessment results and checking in with risk owners to see how treatment plans are progressing.

If the time frames and success measures are slipping away from the plan, make sure that the group is aware that adjustments might be needed. Get them back together again, if needed.

At the end of the time frame, assess the results against the success measure(s) the group selected. Refine the plan and try again if the risk is still in need of treatment.

Step 7:
Communicate the results

When you reach major milestones or the final deadline, tell the team how the plan worked.

If the results weren't what you hoped for, review with the team the gap between your results and the planned measure of success. Do a new risk assessment around the goal (the goal and/or the conditions around it might have changed). Refine your treatment plans based on what you have learned and treat again.

If the treatment was successful in mitigating the risk and helping to achieve the goal, congratulate each other. Share successes and credit with the assessment team as often and loudly as you can.

If what you learned could help others avoid the same risks, work with the team to share its successes more widely as best practices. Consider contacting DES Risk Management so they can share your lessons learned with other Risk Managers.

Find Out More
- The Orange Book: www.hm-treasury.gov.uk/media/3/5/FE66035B-BCDC-D4B3-11057A7707D2521F.pdf
- International Organization for Standardization: http://www.iso.org/iso/home.htm
- Committee of Sponsoring Organizations of the Treadway Commission: http://www.coso.org/default.htm

ERM: A Final Review

ERM: A Final Review

ERM can be a powerful tool in your agency risk management tool kit. ERM is:

- Based on a methodology that is accepted worldwide
- Repeatable, scalable and defensible
- Time specific, allowing for realistic tracking of results
- Success oriented and helps your agency to:
  - Refine goals
  - Improve communication
  - Deploy scarce resources where they will do the most good

Whether you choose to use the seven steps presented here or adjust the method to better fit your agency, remember key ERM principles:

- Risks must be related to goals
- Risks must be assessed and prioritized based on likelihood and impact
- Scarce resources shouldn't be wasted on risks that are unlikely or minor in impact
- "Red zone" risks need a treatment plan. You can:
  - Avoid risk
  - Transfer the risk
  - Reduce the likelihood or impact
  - Accept and monitor
- Risk treatments must fit the risk tolerance of the group (risk appetite)
- Risk treatments should realistically reflect the amount of control you have over the risk
- Goals, risks, incidents and treatments must be reviewed regularly in a blame-free environment

ERM Reporting

ERM Maturity Model

"Maturity model" refers to any scoring tool that measures an agency's progress in mastering Enterprise Risk Management.

Maturity model design takes into account that it requires several years of commitment and practice to achieve the higher levels of maturity. An agency's scores should be expected to increase as ERM programs grow and become more fully integrated into planning and operations.

There are many ways to construct a maturity model, but most are based on an agency's answers to a series of questions. The answers are scored to place the agency along a continuum from beginner to expert ERM practitioner.

Washington has used a specially developed maturity model for state agencies to score their ERM efforts. Called the ERMMM (ERM Maturity Model), it measures ERM progress in four areas. The answers are totaled and the overall results translate to an ERM maturity score on a scale from 1 (no risk management program) to 7 (ERM mastery).

Washington agencies have increased their ERM programs and their maturity model scores significantly over the past few years. Washington is becoming a leader in this area.

Tort Claims

Tort Claims A tort is a civil wrong or wrongful act, whether intentional or accidental, from which injury occurs to another. Torts include all negligence cases, as well as intentional wrongs that result in harm. It is common for the injured party to seek to recover damages.

Tort claims against the state can result from personal injury; bodily injury; property damage, including third-party vehicle collisions; financial loss; or loss of business or damage to reputation, when a claimant believes an injury is the fault of a state agency or employee. With limited exceptions, the state of Washington must pay damages just like a private party when the state or one of its agents commits a tort.

Citizens who ask for information about filing a tort claim should be directed to the website or DES Office of Risk Management (ORM) claims staff for filing information. Tort claim forms and instructions are available on the ORM web site at File a Tort Claim. State employees who want to file a state vehicle accident report or tort claim for an employment-related cause should also be directed to this site.

Once a claim is filed, ORM reviews it to determine who should investigate the claim. Claims may be referred by ORM to the agency where the alleged tort occurred.

The length of an investigation can vary depending on the complexity of issues and availability of documents and witnesses to substantiate causation and damages. When the investigation is completed, the claimant and the agency are notified in writing. If the claim is found meritorious, payment is authorized and issued by ORM in accordance with the findings.

A loss history, or listing of claims filed against each agency, is available from ORM for risk managers to use in planning risk management activities. Quarterly loss reports are provided to risk managers. For other loss history reports, contact Jean.Jelinek@des.wa.gov.

Find Out More ▪ Chapter 4.92 RCW

Self Insurance Liability Program

Self Insurance Liability Program

The state's Self Insurance Liability Program (SILP) is used to pay claims against agencies for auto and general liability losses.

The program is funded by premiums paid by each agency and administered by DES. General and auto claims are investigated and settled through the coordinated efforts of DES, Office of the Attorney General, and the departments of Transportation and Corrections (for DOC-specific claims). Approved claims (including defense costs) are paid by DES from the SILP.

SILP premiums are established by an actuarial formula at the beginning of each biennium. The formula takes into account an agency's claims experience, or loss history (claim payouts) for the previous five years, including pending or open claims.

Risk managers often are involved in investigations and claims determination. They receive copies of all claims filed against their agency. Agencies also receive a quarterly data update of claims that had activity during that period. Find out more at DES Self-Insurance Liability Program.

Certificates of Liability Insurance

You may be asked to provide a certificate of (self) insurance before your agency participates in an outside activity, agreement or lease. These are available at Certificate of Liability Insurance Form.

Agencies purchasing equipment through the Office of the State Treasurer's Lease Purchase Program must also provide evidence of insurance for liability and property damage. At the agency's request, the Office of Risk Management will prepare a written declaration for the state's fiscal agent. Certificates of insurance are available at Certificate of Insurance Request - Lease/Purchase Program.

Both websites provide contact information if you have questions or need help with the forms.

The Retrospective Rating Program

The Retrospective Rating Program

Retrospective rating (retro) is an insurance option available through the Department of Labor and Industries' State Fund (workers compensation insurance). Retro allows participating employers to recover a portion of their workers compensation premiums if they reduce injury rates to employees and lower associated claim costs. Employers may enroll in the retro program individually (if they meet premium size requirements) or form a group of employers (known as a "retro group").

Retro participation, individually or in a group, requires an agency commitment to improve safety and prevent workplace injuries and illnesses to maximize refund potential. If claim costs are higher than allowed in the plan selected, additional premiums will be assessed. If the losses are less than the maximum allowed, agencies receive a partial refund of the premiums paid.

The state's group retro program has operated since 1988. It currently has 44 participating member agencies (yearly enrollment may vary). Participants include medium-sized agencies and small agencies that would be unable to qualify for individual retro enrollment. There are no fees assessed by L&I or DES to participate in the group retro program and 100 percent of the refunds are returned to agencies.

Refunds earned by agencies that participate in the retro program are governed by the requirements of RCW 51.44.170, with preference given to safety and early, appropriate return-to-work for injured employees. Examples of items eligible for a retro refund include:

- Hands-free communication devices
- Digital/security cameras
- Individual first aid/emergency kits for employees
- Adjustable tables, work surfaces or workstations
- Warning signs for use in buildings/grounds
- Non-skid products
- Ice/snow equipment/supplies
- Panic/alert buttons for reception areas
- Card key entries
- Industrial hygiene consultant services
- Specialized lifting devices
- Hard hats, gloves, hearing protectors or respirators
- Safety awards or recognition items
- Commercially produced safety videos or online safety classes or development costs for creating videos
- Attendance at the Governor's Safety and Health Conference

- Subscription to journals or publications
- Membership in a professional safety organization

Find Out More   http://www.lni.wa.gov/IPUB/250-006-000.pdf

Local Government Self-Insurance

Local Government Self-Insurance

The Local Government Self-Insurance Program (LGSI) is regulated by DES. Washington law permits local governments such as cities, counties, special districts and, in some cases, nonprofits to jointly or individually self insure.

To participate, each sets aside a reserve, or pool of monies to pay deductibles. Each may also purchase an insurance policy (called "excess" or "reinsurance"), which helps protects against losses that exceed self-insurance.

Through effective risk management practices, participants can reduce paid losses, which, in some cases, may allow risk managers to retain and invest pooled funds not paid in claims. These funds earn interest and provide a cushion for programs, as the cost of excess insurance is subject to market volatility.

Through monitoring and on-site examinations, the LGSI team from DES helps ensure that self-insurance programs funded with local taxpayer dollars comply with laws and regulations and are financially sound.

Find Out More
- Local Government Self-Insurance Program
- RCW 48.62

Fleet Safety

Fleet Safety

Some state services require direct interaction and contact with citizens at their locations. State employees who deliver these vital services annually log millions of miles in state and personally owned vehicles. Driving safely to these locations is a key component of providing efficient service.

Monitoring vehicle activity is important to every agency with employees who travel on state business. Nationally, vehicle-related fatalities continue to be a leading cause of workplace deaths. Your agency will need help tracking and analyzing auto liability claims, as well as devising policies and training programs to keep employees safe as they drive on state business.

Every state driver is expected to promote safety on the roads by adopting and displaying safe driving habits. The video "Safe Driving Habits: A State of Mind" was created by DES for state agencies to use in new employee orientations for those who drive on business.

The Enterprise Wide Transportation Policy (Enterprise Services Policy No. BR.01.P1) contains statewide policies for travel (Chapter 10) and transportation (Chapter 12) that address safety and risk management policies related to driving and vehicle operation.

Full-Size Passenger Van Safety

Many agencies own or lease large passenger vans. Passenger vans handle and react differently than the typical sedan and drivers need to understand these differences to safely transport passengers.

The National Highway Traffic Safety Administration (NHTSA) has issued numerous van rollover advisory warnings and continues to provide passenger van safety information. Key safety measures advocated by the NHTSA for preventing van rollover deaths and injuries include:

- **Seat Belts** - All occupants need to wear seat belts at all times.
- **Tire Pressure** - Tires should be inspected and tire pressure checked before each use.
- **Driver** - A 15-passenger van should only be operated by trained, experienced drivers who operate these vehicles on a regular basis.
- **Attention** - The driver should be well rested, have restricted cell phone use and conversations with other passengers, and limited drive time (eight hours per 24-hour period).

Federal Passenger Van Safety Resources
- The NHTSA continues to be an excellent resource for the most current information and data about the safe operation of passenger

vans (search word: 15-passenger van) at http://www.nhtsa.gov/.

State Passenger Van Safety Resources
DES requirements and resources for passenger van safety include:

- Statewide van requirements and policies are outlined in Enterprise Services Policy No. BR.01.P1 at 12.60
- A Loss Prevention Review Team Report involving two van accidents (one involving fatalities) issued October 2005 is available at 15 Passenger Van Rollover Report.
- The DES Vehicles and Drivers website contains information, forms, and web links for all state agency drivers.

Find Out More
- DES State Vehicles and Drivers website
- Enterprise Wide Transportation Policy
- http://www.wsdot.wa.gov/
- http://www.wsp.wa.gov/
- http://www.dol.wa.gov/
- http://www.wtsc.wa.gov/
- http://www.dop.wa.gov/Employees/TrainingAndDevelopment/
- http://www.cdc.gov/niosh/topics/motorvehicle/
- http://www.trafficsafety.org/index2.asp
- http://www.nhtsa.gov/
- http://www.iihs.org/
- NHTSA 15-Passenger Van Press Release

Contract Risk Management

Contract Risk Management

Much of the fieldwork of state agencies is carried out by contractors, and contracting involves risk management. Even though agencies procure and award their own client service contracts and have oversight of some personal service contracts, the DES Contract Services Office issues state policies and guidelines to assist those involved in procuring, awarding and managing these contracts.

Before contracting with anyone outside a state agency, agencies are encouraged to assess the risk of that particular contractor using training designed by DES contract experts.

Risk managers may be asked to help with these audits and assessments, to get involved in determining what kind of insurance a contractor must have, or to work on a contractor claim or an incident concerning a contractor.

Find Out More
- Sample Contract Risk Assessments
- DES Contracting and Purchasing Website
- RCW 39.26

Public Records

Public Disclosure
Washington is committed to the principles of open, transparent government. We have one of the most rigorous public disclosure statutes in the nation, with monetary penalties for non-compliance.

Unlike most areas of possible liability at state agencies, fees or penalties related to public disclosure are not eligible to be paid from Self Insurance Liability Program funds.

When an agency is ordered to pay public disclosure penalties, the money must come directly from agency program funds. Most agencies do not budget for this, so these penalties can disturb program budgets. To avoid this, agencies must develop effective public disclosure tracking and response systems and educate all employees on compliance.

State agencies are required to designate a public records officer who is responsible for compliance. Many agencies have located the public disclosure officer with their risk management team. It is not unusual for risk managers to become knowledgeable about public disclosure or to work with their public records officer on issues, planning or training.

Privacy
Some agencies are subject to the requirements of the federal Health and Insurance Portability and Accountability Act (HIPAA), which sets rules for the use, safeguarding and disclosure of health-related information. Those agencies subject to HIPAA must designate a privacy officer, who also may be the public disclosure officer or work closely with the public disclosure officer.

HIPAA violations are investigated at the federal level. They can require considerable staff time and trigger changes to agency processes. If upheld, HIPAA penalties can be large and include criminal prosecution.

Privacy laws mandate certain protections even in agencies not subject to HIPAA. Work with the agency public disclosure officer, privacy officer and data security officer to make sure your agency is meeting its privacy goals and obligations.

Discovery and E-Discovery
Discovery is a legal process in which records are requested in the course of a civil or criminal case. Electronic discovery (often called "e-discovery") refers to any process in which electronic data or records held electronically are sought.

In addition to responding to public disclosure requests, agencies must

be prepared to respond correctly to discovery requests. As with public disclosure, there are mandates on how agencies must respond to discovery requests and penalties possible for non-compliance. Responding incorrectly can result in monetary sanctions, barring of evidence in support of your case, adverse instructions to a jury or a default judgment against the agency.

All agency employees should be aware of their responsibility to:
- Notify supervisors of the need for a written litigation hold directing preservation of all relevant documents, and suspension of routine document retention and destruction policies when they become aware of a reasonable anticipation of a lawsuit.
- Preserve data related to the issue or claim until it can be reviewed with agency lawyers.
- Follow the agency lawyer's preservation-related instructions.

Once the agency receives an official notice that the litigation hold has been lifted, resume normal retention and destruction policies with all records that were kept under the hold.

Records Management

Your organization should have policies and procedures in place for managing its records and information assets. Procedures should address creation, classification, retention, and final disposition or destruction of records. Standardization and consistency are key for maintaining the integrity and accessibility of your public records.

The Office of the Secretary of State's Washington State Archives division publishes state approved records retention schedules that govern how long records must be kept by state agencies and local governments. The State Archives also offers training on records management topics, the Public Records Act, and the Open Public Meetings Act. Your organization's designated Records Manager or Records Officer is the person who is your liaison to the State Archives, and oversees your records management program.

Security Breaches

If confidential information (defined as a person's name in combination with specific data elements such as a Social Security number) from an agency database is inappropriately disclosed (defined as "unauthorized acquisition") through theft or accident, RCW 42.56.590 requires you to notify all affected parties and supply remedies. This must be done quickly after the loss is discovered.

The statute allows anyone injured by the breach to take civil action against the agency. You may be asked to work with the agency privacy

officer and data security manager to develop training, policies or ways to mitigate any losses.

Find Out More
- RCW 40
- WAC 434-615
- http://www.sos.wa.gov/archives/recordsmanagement/Managing-State-Agency-Records.aspx

Worker Safety and Health

Worker Safety and Health

Every agency has the goal of keeping employees safe on the job. It's the right thing to do, makes economic sense for agencies and workers, and is an obligation imposed on employers and employees by occupational safety and health laws.

A high rate of on-the-job injuries increases premium rates for workers compensation. It can also increase the individual rate an agency pays. Although not widely known, a high rate of injuries in an occupational risk class affects the amount each employee in that field contributes to workers compensation premiums. The cost, listed under the category of "medical aid," comes out of employee paychecks.

In Washington, the Department of Labor and Industries has responsibility for enforcing workplace safety and health laws through its Division of Occupational Safety and Health. Each year, it co-sponsors the Governor's Industrial Safety and Health Conference, which alternates between the east and west sides of the state. The conference is a great opportunity to hear state experts and nationally known speakers, as well as tour exhibits of the newest safety resources.

Role of Safety Manager

Agency safety managers regularly meet as a group to share information and discuss common goals and problems. If you are new to state government or to the safety manager role, participating in the group may put you in touch with others who can share resources or be on-call mentors.

Assessing Workplace Safety Needs

The laws that affect workplace safety programs are explained in L&I's safety and health core rules. More specific safety rules may also apply, depending on the nature of work performed by agency employees.

L&I's Form 33 (Safety and Health Program Assessment Worksheet) is a tool for agencies to assess their workplace safety programs and make improvements. L&I provides training on the tool's use and offers assistance with planning and setting up improvements.

Return-to-Work

"Return-to-work" describes the activities that help an injured worker get back on the job. Activities may include working shorter hours, transitional work (original job with lighter physical demands or a temporary, different job) or a modified job (making adjustments to the work site, changing the job to the employee's limitations, or providing tools and equipment).

Helping injured employees return to work as soon as medically possible is a priority for agencies. Studies show that the longer an employee remains off work, the harder it is to return to the original job and income. Returning to work speeds an injured employee's recovery and reduces the financial impact of a workers compensation claim on the employee, the employer and the workers compensation system.

Larger agencies may have claims management or return-to-work coordinators who work exclusively in workers compensation claim management. Smaller agencies may rely on specialists in the human resource area.

See the "Retrospective Rating Program" section for information about a special workers compensation program for qualifying agencies.

Find Out More
- http://www.lni.wa.gov/Main/ContactInfo/
- http://www.lni.wa.gov/IPUB/416-081-909.pdf
- http://www.lni.wa.gov/Safety/TrainTools/Workshops/Available/OSHA300/default.asp
- http://www.lni.wa.gov/wisha/rules/corerules/default.htm
- http://www.lni.wa.gov/safety/basics/Programs/Accident/default.htm
- http://www.lni.wa.gov/Safety/TrainTools/GovConf/default.asp
- http://www.lni.wa.gov/Safety/Research/About/default.asp
- http://www.osha.gov/
- http://www.cdc.gov/NIOSH/
- http://www.asse.org/
- http://www.esc.org/
- http://www.lni.wa.gov/ClaimsIns/Insurance/Learn/Intro/Default.asp
- http://lni.wa.gov/ClaimsIns/Insurance/Reduce/Manage/Ertw/Default.asp
- http://lni.wa.gov/FormPub/Detail.asp?DocID=1493
- http://www.lni.wa.gov/ClaimsIns/Insurance/RatesRisk/default.asp

Employment Liability

Employment Liability

Employee issues can result in poor performance, loss of productivity, grievances, lawsuits or the loss of valuable workers. Employee complaints or lawsuits can become a tort loss and affect agency self-insurance premiums.

All agencies have HR professionals who understand and keep abreast of complex labor laws. These professionals work with agency risk managers to track, analyze and reduce employment liability risk.

The Washington State Human Resources (formerly Department of Personnel) website provides employment liability-related tools, as well as specialized training such as the HELP Academy series.

Find Out More
- DOP HELP Academy
- http://www.hum.wa.gov/
- http://www.ofm.wa.gov/labor/

Glossary

Adjudicate	To make an official decision about a problem or dispute.
Best practice	A business practice or an established way of doing something, developed through experience and knowledge that generally produces positive results in an efficient way.
Certificate of insurance	An official document that gives proof that the person or program is enrolled in an insurance plan/program.
Claim	A formal request that a loss be reimbursed or a person be compensated for a loss.
Claims management	The process of reviewing claims.
Close call or "near-miss"	An occasion when something (generally negative) almost happens.
Commercial insurance	A contract obtained from a for-profit insurance company that provides financial protection against loss, harm or another undesirable event.
Contract	A formal, legally binding agreement for goods or services.
Control	The ability to limit, restrict, direct or manage something.
Discovery	A legal process in which each side of a lawsuit must provide data and/or documents to the other side.
Econometrics	The application of mathematical and statistical techniques to a problem or process.
Electronic discovery ("e-discovery")	A legal process in which each side of a lawsuit must provide electronically stored data and documents to the other side.
Enterprise Risk Management (ERM)	The process of managing everything that could prevent an agency or program from reaching important goals.
ERMMM (ERM Maturity Model)	A tool used to measure an agency's progress implementing the ERM process and practices.

Incident	An event that may result in harm, loss or pose a risk to meeting an agency goal.
Incident reporting	The process of reporting a potentially harmful event to others who need to know about it for response, planning or other purposes.
Litigation	The act or process of bringing a lawsuit against another person.
Loss history	An account of past events, incidents or claims during a specific period of time.
Loss prevention	A process or program to plan and implement actions or programs to reduce risks or the possibility that a loss will occur.
Loss Prevention Review Team	A statutory program authorizing DES to do in-depth reviews of selected incidents and to make recommendations to prevent or reduce losses.
Mitigate	To make the results of an incident less serious or to put plans in place to make a risk less likely to happen or reduce its impact if it were to happen.
Public disclosure	The process of providing public records to requesters in accordance with law and policy.
Records retention	The process of maintaining and storing public documents or data in accordance with law and policy.
Retrospective rating	Also called "Retro." An optional incentive program operated by the Department of Labor and Industries that rewards employers' efforts to reduce workplace injuries and illnesses by returning a portion of premiums.
Return-to-work	A term used to describe strategies for an employee injured at work to return to the job as quickly as medically possible to aid in the recovery process.
Risk	In ERM, anything, big or small, bad or good, that could stop an individual, program or agency from reaching a goal.
Risk treatment	An individual's or agency's response to a risk. In ERM, there are 4 risk treatment options: • Accept the risk and monitor it (generally with a threshold for re-assessing the risk); • Avoid the risk by terminating the program, service or activity; • Reduce the likelihood that a risk will happen or reduce the impact of

the risk event if it happens; and

- Transfer the risk, generally through insurance or a contract.

Risk likelihood or impact	A determination on a 5-point scale of how likely it is that a risk will happen and how serious the impact on the goal will be it if does happen.
Risk map	A chart that graphically displays the combined likelihood and impact scores for each risk to a goal.
Risk register	A list of all the risks to meeting critical agency goals, what treatment will be used to mitigate the risk, the measure of success to apply to the mitigation plan (for example, performance measures) and other key action items related to follow up of a risk assessment.
Root cause analysis	A method of analyzing an event to determine the ultimate cause(s) of the event to make recommendations to avoid similar events.
State risk manager	The risk manager of the Office of Risk Management of DES (RCW 4.92.006).
Tort claim	The process of requesting an agency to make restitution for a claimed wrongful act or omission.
Workers compensation	A program that requires employers to provide coverage for benefits to employees who sustain injuries or illness in the course of their job.

DES Risk Management Contacts

DES Office of Risk Management	Office of Risk Management 1500 Jefferson Street SE Mail Stop: 41466 Olympia, Washington 98504-1466 Fax: 360.407.8022 Phone: 360.407.9199
State Risk Manager	Jason Siems – 360.407.8729
Agency Risk Manager	Craig Ginn – 360.407.9260
Administrative Support	Melynda Campbell – 360.407.8137 Customer Service – 360.407.7935
Claims Unit Investigators	Reginald Cuffee – 360.407.8249 Stephanie Nace – 360.407.8241 Greg Pressel – 360.407.8161
Claims Representatives	Taylor Hildebrand – 360.407.8140 Jordan Frost – 360.407.8286 Cindy Palm – 360.407.8147 Diana Timmons – 360.407.8186
RMIS System Support Team	Tuan Hoang – 360.407.8146 Thanh Ly – 360.407.8145
Loss Prevention	Jean Jelinek – 360.407.8158 Leslie Atkinson – 360.407.9347 Doug Selix – 360.407.8081
Claims Management	Heather Welch – 360.407.9159 Grady Williamson – 360.407-8827
Risk Finance	John Christenson – 360.407.9461 Kimberly Haggard – 360.407.8139
Local Government Self Insurance	Shannon Stuber – 360.407.8153