



# BULLETIN

Volume 11, Issue 1  
July, 2005

Route to:

- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_

**RISK  
MANAGEMENT  
DIVISION:**

**General Information:**

(701) 328-7584  
rminfo@state.nd.us

**Loss Control:**

(701) 328-7582

**Workers Compensation:**

(701) 328-7583

**Office Fax:**

(701) 328-7585

**Website:**

[www.state.nd.us/risk/](http://www.state.nd.us/risk/)

*Risk Management  
Division  
Mission Statement*

*To protect the assets of the State of North Dakota - its people, property, and financial resources - so that the State can continue to meet its obligations to its citizens.*



## Update

Web site:  
[www.state.nd.us/cog](http://www.state.nd.us/cog)

### The RPO/RTO Impact on a Disaster Recovery Business Resumption Plan

To date, in order to develop their COOP plans, State entities have determined whether identified functions are Essential, Vital, Necessary, or Desired. That determination is based on the definitions found in the Process to assist ND State Entities in Developing a Continuum of Government Plan (See the COG web site.) Now it is time for the entities to take the next step – *identifying each business functions' Recovery Point Objective (RPO) and Recovery Time Objective (RTO)*.

In the event of a disaster or audit, entities need to know when they can recover or locate their information. One of the first steps in this process is

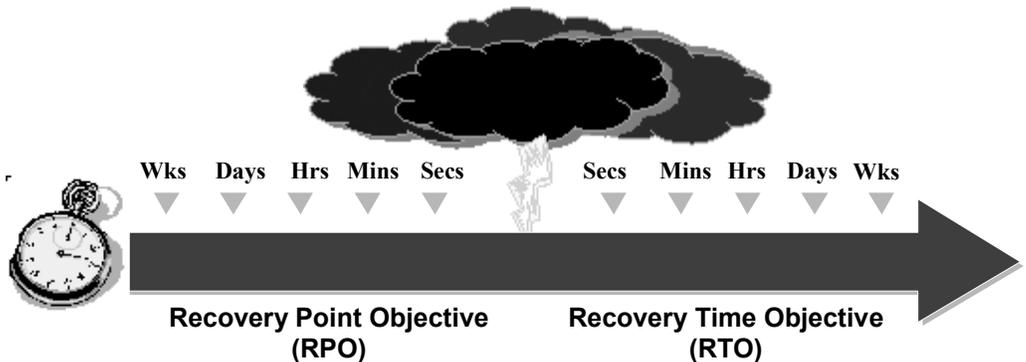
determining the data essential for the survival of your entity's business.

#### How Valuable Is Your Data?

Not all types of data are the same. Most of your organization's data is valuable. Some of it is *extremely valuable and/or absolutely critical to the survival of your entity's business* - **mission-critical** data. The following illustration helps understand the data status rating process.

Mission-critical data would have the shortest RPO. The shorter the RPO, the more current your backup data needs to be. The data that is classified as mission-critical requires up-to-the-minute data currency (the most current data available) to ensure that the recovery point is seconds or minutes, rather than hours, days, or even weeks.

(Continued on page 2)



(RPO/RTO from page 1)

The closer each number is to the disaster, the more expensive the budget cost will be. For example, if an essential function had an RPO of less than one hour, it would be necessary to have the information continually backed up so that the information is mirrored offsite. Naturally, there are IT costs associated with that type of recovery.

The key principle involved is that only those functions that *must be performed because they are key to the survival of the organization* should be listed as a top priority. But remember, the priorities of an agency may change as the duration of the service interruption lengthens. For example, a function that can sustain a delay of 3 days may become a top consideration if the interruption lasts a week.

**How Much Can You Afford to Lose?**

Determining the RPO/RTO formula for an identified function can be defined as:

**Recovery Point Objective (RPO)**

In a disaster you will generally lose data. The *Recovery Point Objective* is the time (relative to the disaster) to which you could potentially recover your data. For example, if you make overnight backups, the recovery point objective could be the end of the previous day's activity.

**Recovery Time Objective (RTO)**

This is the time period after a disaster at which a business function needs to be restored. Different business functions have different recovery time objectives. For example, the recovery time objective for the payroll function may be two weeks, whereas the recovery time objective for issuing a license may be two days.

**Cost of downtime**

A state entity should calculate the potential losses it could incur, both as the result of a down time associated with the disaster and in recreating lost data.

**Balancing the Tradeoffs.**

In an ideal world, organizations would develop backup processes that support up-to-the-minute currency for all their data. In the real world of limited resources, because of the costs involved, this approach just isn't feasible. Organizations must balance the tradeoff between currency of data and investment in resources. Getting this balance right is essential. Under-investing in data currency can result in the collapse of the entity in the event of a disaster. Over-investing in protecting non-critical data can tie up valuable resources better used elsewhere in your disaster recovery and Continuity of Operations programs.

**Continuous Backup Maximizes Data Currency.**

State entities will need to work with ITD to develop and implement appropriate backup technologies and processes once data has been classified according to Recovery Time and Recovery Point Objectives. For the most critical data with the shortest RPO, a solution such as electronic vaulting that supports continuous backup will need to be implemented. Unlike periodic backup processes that ensure recovery of data only up to the point that the backup was done, continuous backup closes the window for potentially lost data. While you can never absolutely guarantee zero loss of data, continuous backup solutions can minimize data loss to minutes or even seconds.

**Data recovery budget.**

The following criteria can assist in determining the criticality of business functions. There may be others that are of importance to a State entity.

- ♦ Maintenance of public health and safety.
- ♦ Income maintenance for citizens.
- ♦ Income maintenance for government employees.
- ♦ Payments to vendors for goods and services.
- ♦ Requirements for compliance or regulation.

(Continued on page 6)



*Loss Control Tools*

Updated

**Inspection Checklists & Inspection Form**

The inspection checklists and form found in Section 4.3 of the Manual have been revised in order to directly correlate with the RM Fund Discount Application #7a, documentation of corrective action for deficiencies identified in facility inspections. You will find that the last column of the inspection form has an area to record what corrective action has been taken to correct the problem identified during the inspection, the date it was corrected and the initials of the person that took the corrective action or that is documenting the corrective action. This is an area that is often forgotten or not completed by the inspector, but can create liability as the documented deficiency is an identified exposure left unresolved. Therefore, it is important to close the loop on this process.

Like everything else, inspection requirements can change. Therefore, the checklist itself has also been updated and reformatted. The updated checklists and form can be found at [www.state.nd.us/risk/publications/docs/chap04.pdf](http://www.state.nd.us/risk/publications/docs/chap04.pdf). Go to the link to print and replace Section 4.3 in your RM Manual.

**Limitation of a Vendor's Liability**

As we have stressed for a number of years, a critical loss control tool for State entities is proper contract management. Along with the importance of drafting appropriate indemnification and insurance provisions, because most state employees have no authority to comply, we have cautioned against agreeing to language

(Continued on page 5)

## RM Fund Discount Program – Raising the Bar



The review of the Risk Management Fund FY '06 contribution discount applications has been completed. The number of applications submitted for this, the fourth year of the discount program, were almost equal to last year's number. Of the 48 applications 12 entities qualified for the full 10% (with many others near 10%). The discounted savings realized totaled \$56,110 out of a potential \$133,869.

**Congratulations** to those of you who saved money on your entity's contribution! Risk Management appreciates your proactive efforts to reduce exposures and losses to the State. Risk Management's mission is to protect the assets of the State and that mission cannot be accomplished without your help in creating and participating as members of a strong loss control team!

Although some of the entities will be pleased with their discounts, we suspect that there will also be some that will be disappointed due to the more stringent review. Because of the number of entities that have accomplished the full discount and have established their loss control programs to meet the criteria of the discount program, we know that it is possible and that information about the program is being disseminated correctly. Therefore, we ask that you continue to forge ahead and use the resources that are available to you and your entity to achieve the full 10% next year. (In particular, see RM Schedules for Portions of Committee Meeting Agendas Specific to Qualifying for the RMF and RMWCP Discounts at page 2.6-4 of the RM Manual.)

### That Which Gets Measured Often Gets Done . . .

The RM's discount programs are functioning as safety incentive programs that put the reward emphasis on "leading indicators" (proactive) rather than "trailing indicators" (reactive). What this means is the focus is on those activities, behaviors, processes, etc. that lead to results (i.e. attending and documenting training) rather than on the end results (i.e. decrease in the number of claims). To some extent, a system using the trailing indicators already exists through the entity contribution billed each year which takes into account the entity's loss history. Since the inception of the Fund, emphasis has been put on the front end through loss control. The discount programs were put into place merely as a bonus to reward entities for changing their culture and shifting their focus to action-based performance through the leading indicators that have been outlined in the discount program application.

Accountability and tracking is a key component to an incentive program like the Fund's. RM has limited staff and resources like every other entity in the State and therefore, is not able to conduct a physical audit and inspection of each entity for each year's discount. The only alternative is to establish a consistent and reliable method of accountability and performance management via documentation and records. Through

the discount programs, RM has identified certain risk-reducing and compliance-related activities that have proven effective for the principle areas of risk control, loss prevention, and regulatory compliance. By documenting the activities and tracking completion, RM is able to proactively work with the entity contacts to promote key risk management activities and ensure completion in a timely manner. As these efforts of the entity reduce losses, RM in turn is able to reward that entity with a lower contribution.

Some dollars used to pay contributions to the RM Fund are federal dollars which means the federal government audits the Fund expenditures annually. Because the discount program results in fewer dollars available to the Fund to pay claims, RM has to provide documentation that ensures the discount program doesn't lose credibility and become merely an ineffective exercise in paperwork.

### Tips to keep in mind for the FY '07 Discount

The common shortfalls for not qualifying for the full discount this year are easy fixes. One that appeared often was the lack of follow-up in the minutes. For

example, in a January meeting, a member mentions compliance with the records retention schedule and reports that he/she will either bring the entity coordinator to the next meeting or check with the coordinator on the status and report on compliance at the next meeting. However, the issue is never mentioned in future meeting's minutes. The actions were so close – but just didn't close the loop! The sure-fire way to avoid this shortfall is by reviewing the minutes before preparing the agenda for the next meeting. The follow-up tasks should be added to the agenda as an action item, along with the member's name who was assigned to the task.

Another shortfall is the minutes lacking substance. When this happens, the meetings appear to be superficial and clearly do not serve the intended purpose. This could happen because thorough minutes of the meetings were not taken or the meetings were not operating effectively and in compliance with Section 4 of the RM Manual. The LCC meeting can certainly include functions of other committees, such as quality control, as long as the majority of the committee and meeting activities demonstrate a risk management loss control program. Unfortunately, an entity cannot get past #1-4 of the application unless the minutes reflect an "active" LCC meetings and that the committee is conducting applicable loss control functions.

Credit for #5 which addresses Employment Practices Liability (EPL) exposures is often lost because the policies are not specified (the statement 'risk management training/policies' is not sufficient); the minutes do not explain how each policy is communicated to all of the employees and how that communication is

The RM's discount programs are functioning as safety incentive programs that put the reward emphasis on *leading indicators* (proactive) rather than *trailing indicators* (reactive).

documented; copies or a sample copy of the documentation piece is not provided (acknowledgment statement, training sign-in sheet, etc.); it is not reported how the process is monitored to ensure compliance by all employees; there is a failure to describe each division/department's procedure and that each one is in compliance (each dept. needs to be listed, confirmed, and described separately in the minutes); Drug-free Work Policy (Act of 1988) is offered as an equivalent of a Substance Abuse Policy; and there is a lack of customization or documentation of the emergency based policies for each division/department/office of the entity. EPL continues to be the most costly exposure for the RM Fund and can be dramatically impacted by EPL loss control procedures addressed under #5.

Without question, #6 dealing with review of incidents and accidents was one of the highest contenders for noncompliance. RM has been aware of the difficulties complying with this criterion and has provided information on the issue through Bulletins, recommendations, and Seminar presentations. Because compliance requirements are set by statute, we have little leeway or discretion in valuing this criteria. For these reasons, you will find that the documentation and structure are very specific and without certain requirements met in your LCC meeting's minutes, they cannot be considered compliant. To help your entity meet the requirements, we have posted on the RM website the PowerPoint presentation *Guidelines for Conducting Loss Control Committee Meetings* and the *Loss Control Committee sample document/forms*.

The purpose of criteria #6—the reason for holding an executive session—is fundamental to effective loss control. This is the time during a LCC meeting that the members of the LCC can discuss the entity's incidents/accidents/claims/lawsuits freely to determine the root cause of the incident or possible trends. The discussion held during an executive session is exempt from the open records law—in other words, members cannot be questioned about the information they discuss during an executive session. This is important because the members may discover through the review such things as a trend in certain incidents; that an incident was caused because an employee was not trained properly; or that an incident was caused because an outdated policy was in place. This is the Loss Control Committee's chance to get to the nitty-gritty of each incident and build awareness within the group of what incidents may be costing the State.

Once all of the incidents are discussed, the executive session can be closed properly. If it was decided in the executive session that, for example, a policy must be changed for a specific person to monitor a portion of a sidewalk and to apply ice melt when certain conditions arise, that change in policy should be discussed and documented in the reopened portion of the meeting—*without referencing specific claims or incidents*. Of

course, members should be assigned to carry out these actions and report on the progress in future meetings. *Remember* that the details of the incidents discussed in executive session need to stay there – do not repeat the details (names of injured, numbers of types of claims, etc.) in the open session – that will cause that incident to become an open record. Keep the record 'general' when discussing the appropriate 'actions to be taken'. Also, remember, loss reports distributed to the LCC members for discussion should be collected and shredded after the meeting.

**NOTE:** The statutory authority in the form language has been updated to reflect reference only to the applicable sections of the Tort Claims Act (N.D.C.C. ch. 32-12.2). Make sure you update your forms to reflect the appropriate language.

Another shortfall identified is criteria #7a discussing the inspection checklist. Inspections may be conducted, but the LCC minutes fail to document if/what/when corrective action was taken to address the deficiencies and/or the checklists fail to document the corrective action. We hope that the revised inspection checklists found in Section 4.3 of the Manual will help address this shortfall.

It was surprising how the new criteria #9 addressing contractual risk management compliance appeared to be confusing to some entities. This criterion is procurement based and can be addressed in a similar manner as #8 - either by having the procurement contact in your entity report in a LCC Meeting or assign a member to get that information from the procurement contact and report back to the committee. There are several elements that are required in order to consider your entity compliant for criteria #9 including training provided by the Procurement Office (details can be obtained from Procurement). It is also important for your entity to have a policy incorporating this criterion.

Finally, read the Application, go through it carefully, and document the criteria in the Minutes (or other means) as if the person reviewing it has no prior knowledge of the entity's policies and procedures. Each year the documentation should provide answers to the application as if the reviewer is seeing it for the first time – RM cannot credit activities documented with previous applications. There really are no trick questions or hidden criteria. Utilize the tools that are available and posted on RM's website to achieve the full discount.

And last, but not least, use the resources available through the RM web site, previous Bulletins, and **call with questions** – the Risk Management staff remains dedicated to see that your entity achieves a 10% discount! **Good Luck!!**

(Continued from page 2)  
 proposed by vendors that would either indemnify the vendor or limit the vendor's liability. Because of that lack of statutory authority, in the past entities were often able to negotiate those requests away. Recently, however, some vendors have taken the position that unless there is some limitation of their liability, they will not agree to sell the State software, communication, and electronic equipment. Often they attempt to limit liability to the cost of the contract - sometimes a minimal amount.

Working with the offices of the Governor and the Attorney General we were able to get legislation passed this last session so that if it is determined to be in the best interest of the State, and if the negotiated terms are approved by the Attorney General and the Director of OMB, state employees do have the authority to limit a vendor's liability. (Senate Bill 2250).

This authority, however, does not mean that we should not continue to try to get the vendor to waive the requirement to limit its liability. But, if those negotiations fail, application can be made to limit the vendor's liability by submitting SFN form 54345 to either the Office of the Attorney General or OMB. The application will then be reviewed by ITD to determine whether or not there is a potential negative impact on other State computer data, software or programs. If ITD determines no such impact is probable, the application will be reviewed by Risk Management to see if the negotiated level of limitation of the vendor's liability is appropriate. To assist you in your negotiations, a 2004 report from the National Association of State Chief Information Officers (NASIO) determined that generally the accepted amount of liability in relation to the value of the contract is two times the amount of the contract. Higher limits would be warranted for high-risk contracts. Do not hesitate to contact our office for help with your negotiations.

## RMWCP Update



### Designated Medical Provider -

With the start of a new discount year on July 1, 2005, it is time to update your employees' DMP forms. To qualify for next year's discount, a copy of the list of your entity's employees who have opted out of our chosen DMP and selected a different provider for FY'06 is due in our office by September 1, 2005.

**Online Incident Reporting -** As discussed at this year's spring seminar the new Risk Management online incident reporting system (Risk Technologies) is up and running. You are encouraged to become familiar with the system and use it to report all incidents. Recently WSI has also put an incident report form on their web site. To ensure our incidents are

protected by state statute, are trackable in our system, and to qualify for the Risk Management discount, you MUST use the Risk Management incident reporting forms. Please do not send incident reports to WSI.

**Corresponding with WSI -** Just a reminder, should you have a concern about a claim and want to provide more information on the claim to WSI, all correspondence (other than the FROI) must first be forwarded to our office. As all State entities are under one account, with our office as the contact, it has been creating some confusion and extra work for WSI when they receive information from different sources. Your cooperation in this matter is appreciated.

## Introducing NotiFind



The State COG Team made a decision to purchase an emergency notification system called NotiFind that interfaces with the State's continuity planning software, LDRPS. NotiFind will facilitate quick and effective contact with key personnel in the time of an emergency, deliver critical messages, provide important data for the operation of the State's COG and COOP procedures, and establish a toll-free Message Center where contacts can listen to messages such as location-specific alerts and emergency information. Learn more about NotiFind at the upcoming COG/COOP training.

## COG/COOP Training for LDRPS, NotiFind and BIA

July 18 beginning at 8:00 a.m. through noon on the 20th was the initial LDRPS, NotiFind, and BIA training. More sessions will be scheduled for August and September. The format of the training is—the first 6 hours will be a LDRPS refresher; the rest of the first day will be training on NotiFind; and the following day and a half is devoted to BIA (Business Impact Analysis).

The July session was held at the Corporation and Continuing Education Computer Lab at the BSC Student Center in Bismarck.

Check the COG web site at [www.state.nd.us/cog](http://www.state.nd.us/cog) for upcoming August and September training dates and locations.

Register by contacting [jquinlan@state.nd.us](mailto:jquinlan@state.nd.us) or [rheller@state.nd.us](mailto:rheller@state.nd.us).

## Risk Management Division

Century Center  
1600 East Century Avenue, Suite 4  
Bismarck ND 58503-0649

### CHECK IT OUT!!

Please check your address label.  
Report any corrections to our office.

## BULLETIN

(RPO/RTO from page 2)

- ◆ Effect on state government cash flow.
- ◆ Criticality Classification.
- ◆ Effect on production and delivery of services.
- ◆ Volume of activity and recovery costs.
- ◆ Effect on public image.
- ◆ Inter-system dependency.

The following categorization is suggested as a means for classifying computer application systems used by an agency:

- ◆ Must be processed in normal mode; no degradation is acceptable.
- ◆ Only high priority; e.g., high dollar item transactions or critical reports will be processed.
- ◆ Processing will be carried out on a "time available" only basis.
- ◆ Processing will be suspended, but data collection will continue.

- ◆ No processing or data collection will be carried out until normal computer capacity is reestablished.

### Conclusion

State entities carry out hundreds of operations that management and staff consider important. Key resources may be unavailable during a disaster. *The entity must concentrate its resources on those operations that are most important for public health, safety, and the welfare of our citizens.* The aim of a disaster recovery/business resumption plan is to reduce potential losses, not to duplicate a business-as-usual environment.

References: Iron Mountain Limited and Iron Mountain Inc.

### The State COG IT Legislative Committee Large Project

Because the IT Legislative Committee Large Project requirements for the State's continuity of operations plan software have been met, the COG Team decided at its June 27, 2005 meeting to start the Project's close out procedures.

As a part of that close out, Janell Quinlan, the Project Manager will be developing a survey that will be sent to some agencies to complete. If a survey is sent to you, we would appreciate your prompt participation so that we can complete yet one more milestone in the continuity of operations planning process.

Thank you for all of your help in getting us to this point in the process.