



Recovery and Mitigation for Transportation Management Centers

Final Draft Technical Document

February 2007
Report No. DTFH61-01-C-00181

Notice

This document is disseminated under the sponsorship of the U.S. Department of Transportation in the interest of information exchange. The U.S. Government assumes no liability for the use of the information contained in this document.

The U.S. Government does not endorse products or manufacturers. Trademarks or manufacturers' names appear only in this report only because they are considered essential to the objective of the document.

Quality Assurance Statement

The Federal Highway Administration (FHWA) provides high-quality information to serve Government, industry, and the public in a manner that promotes public understanding. Standards and policies are used to ensure and maximize the quality, objectivity, utility, and integrity of its information. FHWA periodically reviews quality issues and adjusts its programs and processes to ensure continuous quality improvement.

Report No.	Government Accession No.	Recipient's Catalog No.	
Title and Subtitle Recovery and Mitigation for Transportation Management Centers		Report Date February 2007	Performing Organization Code
		Performing Organization Report No.	
Author(s) Andrew Iserson – Telvent Farradyne		Performing Organization Report No.	
Performing Organization Name and Address Telvent Farradyne Inc. 3206 Tower Oaks Blvd. Rockville, MD 20852		Work Unit No. (TRAIS)	Contract or Grant No. DTFH61-01-C-00181
		Type of Report and Period Covered Final Report December 2005 – February 2007	
Sponsoring Agency Name and Address Office of Transportation Management Federal Highway Administration 400 Seventh Street, S.W. Washington, D.C. 20590		Sponsoring Agency Code	
		Supplementary Notes Raj Ghaman, FHWA Office of Operations, Research, and Development, FHWA Project Manager	
Abstract This document presents the issues involved with system outages in Transportation Management Centers (TMC). It proceeds through defining system outages, gaining appropriate management support for the issues, cost/benefit for mitigation of system outages, preparing for a system outage, best practices, ongoing testing and maintenance of the plan. Chapters within the document include: Recovery and Mitigation in the TMC, Synthesis of Current Practices, The Planning Project, Recovery and Mitigation Policies, Mitigation, Testing Preparedness, Ongoing Support for the Plan, and Summary including activity checklists.			
Key Words Traffic Management Center, TMC, Recovery, Mitigation, Continuity of Operations, COOP, Disaster Recovery, DRP, System Outages		Distribution Statement No restrictions. This document is available to the public through the National Technical Information Service, Springfield, VA 22161.	
Security Classif. (of this report) Unclassified	Security Classif. (of this page) Unclassified	No. of Pages 115	Price

TABLE OF CONTENTS

RECOVERY AND MITIGATION IN THE TMC: DEFINITIONS AND PURPOSE.....	1
Overview of Recovery and Mitigation.....	1
Effects of Outages	2
Reasons for Planning.....	2
Overview of the Document	4
Functions of a TMC	4
Importance of Recovery and Mitigation for a TMC.....	6
Types of Mitigation	7
Alternate Sites.....	8
Documentation.....	9
Testing	9
SYNTHESIS OF CURRENT PRACTICES.....	11
State-of-the-Art	11
Management’s Commitment	11
Policy Issues	12
Planning.....	14
Testing	17
Documentation.....	17
Alternate Site.....	19
State-of-the-Practice	20
Management Commitment	20
Policy Issues	21
Planning.....	22
Testing	25
Documentation.....	25
Alternate Site.....	26
Synthesis of Results & Best Practices.....	26
Responding to Actual Emergencies.....	26
Communicating Information about the Outage	28
Areas Normally Overlooked.....	28
Businesses Unable to Operate	29
Results of Survey Questions and Interviews	29
Actual Experiences.....	32
Best Practices.....	33
THE PLANNING PROCESS	43
Overview of the Planning Process	43
Planning Generically for All Types of Outages.....	44
Team.....	46
Management	48
Documentation.....	48
Communications Infrastructure	51
Alternate Sites.....	52
Risk Mitigation.....	54

Funding and Approvals for Planning.....	60
Continuity of Operations.....	61
Testing of the Plan.....	63
Ongoing Support for the Plan.....	64
RECOVERY AND MITIGATION POLICIES	67
Policy Issues	67
Internal Communication Policies	68
External Communications Policies.....	70
Decision Making Policies for Outage Management	70
Policies for Setting Priority by Length of Outage	71
Policies for Setting Priority for DRM Planning	72
Policies for Ongoing Plan Maintenance & Updates	73
Succession Planning Policy	73
Risk Mitigation Policy.....	73
Returning to Normal Conditions	74
Planning for Returning to the TMC.....	74
Timing of the Return to the TMC.....	74
Implications of Being at an Alternate Site.....	75
TYPES AND CAUSES OF SYSTEM OUTAGES AND RELATED RECOVERY AND MITIGATION.....	77
Mitigation.....	77
Loss of Infrastructure.....	77
Loss of Key Personnel.....	79
Loss of Computer Systems	80
Community-Wide Disasters	81
Mitigation of Risk for Periods of Recovery	83
TESTING PREPAREDNESS	87
Purpose of Testing the Plan.....	87
Beginning the Test Planning Process.....	89
Types of Testing	91
Timing of Tests	92
Review of Testing	93
ONGOING SUPPORT OF THE PLAN	95
Management Commitment.....	95
Commitment of Ongoing Support of Plan	96
Prioritization of Documentation	98
SUMMARY	99
Project Initiation	99
Project Initiation	99
Business Impact Analysis.....	100
Project Funding.....	100
Project Funding.....	100
Recovery and Mitigation Planning	100

Recovery and Mitigation Planning	101
Recovery Team	101
Recovery Teams	101
Mitigation.....	102
Infrastructure Mitigation.....	102
Network Mitigation	103
Telecommunications Mitigation.....	103
Mitigation Policies.....	104
Testing Mitigation	104
Recovery.....	104
Documentation.....	104
Recovery Policies	105
Alternate Site	105
Recovery Supplies	106
Recovery Processes	106
Recovery Testing.....	107
Support for Personnel During a Recovery.....	107
Field Devices	107
Return to the TMC.....	108
Return to TMC.....	108
Plan Review	108
Trigger Events to Review Plan	108

1

RECOVERY AND MITIGATION IN THE TMC: DEFINITIONS AND PURPOSE

Chapter 1 Purpose:

Identify the reasons that recovery and mitigation are important to the reader and the reader's organization. To set a proper reference point, a definition of the problem, size, and effect of recovery and mitigation as used in this paper will be set. Recovery and mitigation will then be brought to a personal level with discussions about levels of and reasons for preparedness, levels currently being employed, and specific needs of Traffic Management Centers (TMC).

Chapter 1 Key Message:

- u Recovery and mitigation are critical to the TMC organization
- u The approach to recovery and mitigation strategy is based on the specific organizational functions and criticality of operations
- u Recovery and mitigation is made up of a number of different activities which can vary from agency to agency with no set formula. Each needs to be considered in relation to the specific recovery and mitigation strategy.

OVERVIEW OF RECOVERY AND MITIGATION

Operation centers throughout the governmental and business worlds frequently pay little attention to the processes to be handled in the event of a system outage. Frequently, management has more priority issues on their plate than can reasonably be handled. Recovery and mitigation, also known as disaster recovery or contingency planning, is a topic that is normally relegated to the position of being important, but not quite as important as other issues on the list of priorities. That is, until a significant stoppage occurs. For the more fortunate management, the stoppage that becomes the wakeup call will occur within an operation center other than theirs. Outage war-stories that are reported in the press and circulated through the profession may serve as the wakeup call. Whatever the reason, this wakeup call is critical for all operation centers, including Transportation Management Centers (TMCs).

Recovery and mitigation of operational systems are serious and important considerations for all organizations. Operational systems that are made up of hardware, software, people, facilities and procedures, are exposed to a myriad of possible causes of stoppage. Stoppages of some type are inevitable and will happen. Responsible management must review the services provided by their operations with an eye towards the effect of loss of those services. Based on this analysis, a decision must be made as to the investment that should be made in mitigation of possible stoppages and planning for recovery of operations should a stoppage occur.

Emergency preparedness and response funding was set at \$6.5 billion in President Bush's FY2007 budget recommendations. This budget acknowledges the extent of the problem that may occur due to terrorism, fires, civil disturbances, weather, sickness, systems viruses, and the like. Of 500 corporations recently surveyed, over 90% acknowledged security breaches in their systems alone.¹ This is a realization that system stoppage is not a question of "if", rather a question of "when".

Effects of Outages

Systems outages within TMCs may be caused by a number of issues, including but not necessarily limited to human error, equipment failure, natural disaster, loss of infrastructure, loss of staff, an area-wide crisis, or cyber terrorism. Cyber terrorism alone has increased organizational outages. The Computer Emergency Response Team (CERT) reports a 500% increase in security incidents between 1999 and 2001.² No matter the cause of the outage, the effects will be the same – a TMC will not be able to perform the work necessary in order to meet their commitments to the community. In the case where additional responsibilities are given to the TMC during periods of community-wide incidents, these are also not executed. Other effects that are less obvious include the community and stakeholder's loss of confidence in the TMC and related loss of reputation of the organization.

Systems are not simply computer hardware and the software that it runs. Systems within the TMC may be automated, manual, or a combination of the two. Traditionally, contingency planning has been based around automation, determining the course of action for the loss of the computer infrastructure. Unfortunately, the mission of a TMC can not be accomplished if any of the other parts of the system are not available for use.

Staffing is key to the systems that are running within a TMC. Many TMC functions are performed as manual processes while others are performed as a combination of man and machine. A "lights out" operation where the computers are running without people present is normally considered science fiction. As such, the loss of key staff members or the loss of a significant number of staff members can affect an operational outage.

Outages may be caused by a loss of facilities. Loss of use of the building occupied by the data center or important components of the building infrastructure creates an outage situation. These include such things as structural issues, inability to enter the building due to strikes or riots, loss of electricity, loss of water, air quality issues within the building and suspicion of an impending incident.

Underlying TMC hardware, software, people and facilities are the processes. Normal conditions and those that are out of the ordinary should be covered within approved, documented, and trained processes. System outages may be avoided by having complete processes that are understood by all parties.

Reasons for Planning

As is true with any organizational decision, a quantitative assessment should be made of the value of recovery and mitigation of operational systems as it relates to the goals of the organiza-

***This is a realization
that system stoppage
is not a question of
'if', rather a question
of 'when'.***

tion. The ultimate decision of the size, complexity, and need of a plan will be different for each organization. Decisions may also be different for each system within an organization. Costs for recovery and mitigation of systems are based on the length of time that the system may be unavailable and the integrity of the data leading up to the system stoppage.

Depending upon the organizational goals, effects of a system outage may be anywhere on a spectrum from little to a major community issue. The investment in recovery and mitigation should be dictated according to the analysis. As will be covered later in this study the significant factors that need to be considered is the amount of time for which there can be an outage of the systems, and the currency of the data being in the system when the system is working again. Once these two factors are analyzed, a management decision can be made on the budget to allocate to recovery and mitigation within the organization.

It must be remembered that daily disk drive backups and the use of virus protection should not be considered a recovery and mitigation plan. They may be part of a plan, but these alone do not constitute a plan in and of themselves.

Recovery and mitigation planning may provide advantages to the TMC in addition to the insurance of being prepared for a disaster. In putting together a recovery plan and a mitigation strategy, management may take advantage of costs savings that are associated with better managed systems assets. Part of the planning process requires inventorying the assets. The inventory allows reproduction of the environment as necessary. Inventorying of these assets will allow management to assure that proper numbers and levels of assets are accounted for and maintained. It is likely that during the planning process a different number of required assets will be determined than have been allocated.

The analogy of a recovery and mitigation plan being equated with an insurance policy is an accurate comparison. In both cases, the investment is being made with the hope and expectation that it will never have to be used. If it has to be used, any and all money spent was well worth the investment. If an outage is not spent the fortunate agency may then question all of the efforts and expenditures that were made in their recovery and mitigation efforts.

The end result of a recovery and mitigation project is the ability to circumvent some problems that would otherwise create a systems outage. In the case where outages are not able to be circumvented pre-established, pre-approved methods for to manage the outage situation are in place and understood. IBM suggests that "Predictability of the reaction to a disaster is the goal. This can be accomplished by having a combination of automation functions and well documented and regularly tested procedures. In other words, you do not want to wait until a disaster occurs to find out whether or not your plan will work."³

Traffic Management Centers (TMC) are different in every aspect of their operations. Differences begin with their organizational goals and objectives. It continues on to their management style and operational procedures. The organizational differences result in significantly different recovery and mitigation needs within their area.

TMCs vary from not understanding the need or complexity of recovery and mitigation to having a well thought out and effective program. The reasons for differences in the knowledge of and is often attributed to a lack of funding or lack of prioritization for this type of program.

Few TMC managers reported a systemic approach being used in order to determine related recovery and mitigation efforts. In designing a recovery and mitigation strategy it is important to

focus it correctly so that needed procedures are in place, while keeping them to the minimum required. The level of recovery and mitigation is frequently based on what seems to be the right answer whether that is doing daily backups or having an alternate site sitting in wait for a stoppage. The only influences that are universal among TMC managers is the scarcity of funding and the number of top priorities imposed, both of which have the affect of pushing recovery and mitigation planning further down the list than may be appropriate.

OVERVIEW OF THE DOCUMENT

The document is presented in a manner that will be useful for TMC or other operations center managers. It presents the reasoning behind recovery and mitigation for TMCs and the necessary steps for preparing, testing, and supporting a recovery and mitigation plan in the following chapters:

- u Chapter 1: Presents an overview of recovery and mitigation, TMCs and the importance of recovery and mitigation efforts for a TMC.
- u Chapter 2: Provides a synopsis of current practices, including state-of-the-art and state-of-the-practice. Lessons learned from TMC practitioners are also presented.
- u Chapter 3: Is a summary of planning for many types of outages. The process is presented generically, providing the opportunity for users to tailor it to their needs.
- u Chapter 4: Reviews policies that could be used by agencies to facilitate recovery and mitigation practices. Also discusses strategies for implementing policies.
- u Chapter 5: Presents the types and causes of systems outages and describes how and why they may occur along with the potential mitigations.
- u Chapter 6: Describes the testing process, particularly types of testing, why it is needed, and how to plan for, implement, and review the process.
- u Chapter 7: Presents support material for recovery and mitigation efforts and ongoing documentation upkeep.
- u Chapter 8: Provides a summary of the previous chapters through checklists for each of the major efforts. Each checklist item is referenced back to a specific section in the document.

FUNCTIONS OF A TMC

Functions of a TMC vary greatly depending upon needs of the community, funding, political pressures, philosophies of management, environmental concerns, and the like. During a community-wide emergency situation, functions provided and prioritization of various functions may also change. The TMC may be required to assist in evacuation efforts for the community. Resources available to the TMC can be used to help inform the community of important information, thus making them a focal point of distribution of information. These functions have the effect of changing recovery and mitigation necessities as well as functions of the TMC.

The TMC is uniquely able to monitor changing conditions within a municipality and assist in interagency communications during periods of emergency situations. Through the use of the existing infrastructure of cameras and sensors needed to monitor the roadways the TMC may assist

other agencies by notifying them of changing conditions. Help may be provided with functions such as routing of emergency personnel and establishing prioritized approaches to cleanup.

The operations centers occupied by many TMCs are well suited to act as an interagency communications conduit during times of emergency. The structures and procedures may have been designed for high availability in the event of an emergency situation. Buildings may be hardened with redundant power and communications facilities. In being at the table during planning and execution of emergency plans the TMC can also assist by providing up-to-date information on status of effected areas.

Surface transportation and thus the TMC are vital to the ongoing health of the community. Free flowing surface transportation is required for a vibrant economy. Quality of life changes dramatically when surface transportation is adversely effected as lack of free flowing surface transportation results in less free-time for drivers as well as changes in the pricing and stock levels of consumables. Air quality also tends to degrade when vehicles lack the ability to freely move on the roadways.

The importance of the nation's roadways to the wellbeing of the community cannot be underestimated. Trucks are a major component used to supply goods to the market. Without these goods appropriately supplied, both the community's economic base and quality-of-life are adversely affected.

Congestion in surface transportation has significant ramifications to our communities. Significant congestion results in less free-time for drivers to spend with their families. Elected officials throughout the country frequently speak to the issue of congestion and possible solutions making this a significant issue to address. Congestion on our roadways may also results in degraded air quality due to standing vehicles emitting toxic substances at idle.

As is true with the basic functions of TMCs, functional requirements of individual TMCs during emergency situations differ. Of primary concern to most TMCs during emergency and non-emergency times is the safe passage of people through the area. During emergency situations this becomes more complicated and may include evacuation of the populous. Safe movement during emergency situations may include additional traveler information being supplied both to help the flow of traffic and to keep people calm in the face of the emergency. The emergency situation may require the movement of goods, personnel and equipment into the area to secure and stabilize the situation. The TMC may have a role in movement of this type of national security assets into the area as well as monitoring of additional threats to the community.

The National ITS Architecture has identified the use of a TMC during emergency situations as a critical element. It includes an Emergency Management Subsystem which addresses many of the significant emergency issues that affect the highway system and our communities. The subsystem addresses the following issues.

- u Emergency routing – the coordination of emergency vehicles with the traffic management system.
- u Road closure management – the closing of roads necessitated by safety and other conditions.
- u Transportation infrastructure protection – monitoring of critical pieces of transportation infrastructure for potential threat conditions.

- u Wide-area alerts – alert the public of significant issues.
- u Early warning System – alerts public of potential disaster conditions.
- u Disaster response and recovery – support for emergency response plans.
- u Evacuation and reentry management – supports evacuation and reentry of the citizenry in case of an emergency situation.
- u Disaster traveler information – providing traveling information to the public during emergency situations.

As an objective, establishment of a recovery and mitigation plan that will support the community in these ways during emergencies should be considered.

During the September 11, 2001 attack on the World Trade Center and Pentagon, the Virginia Smart Traffic Center (STC) in Arlington, VA was able to use their ITS infrastructure to improve traffic flow, assist in protecting strategic locations, and support delivery of emergency services. In using signal timings patterns that are normally used to allow vehicles to quickly leave Washington, DC after July 4th festivities the STC facilitated those leaving the area. HOV lanes were changed to an outbound pattern and made available to all vehicles. Emergency services delivery was also assisted by information from the STC.

Information dissemination has been reported to be vital to success during emergency situations. Emergency responders need to share information between each other in order to efficiently and effectively handle the situation at hand. The TMC can facilitate this exchange of information and data between various governmental agencies, both within the municipality and also regionally.

Public information will assist in keeping the citizenry calm. Communications to the public may include the use of the media as well as the installed ATIS communications conduit. Emergency information as well as the condition of the roadway infrastructure should be communicated using these facilities.

During emergency situations the movements of people and supplies into the area is vital to stabilizing the community. People and supplies are needed in area in order to rebuild and re-supply the community. The restoration of the normal flow of goods and supplies to the general public is needed quickly after the emergency situation has abated.

The TMC may also be looked at to monitor the critical highway infrastructure for the possibility of additional threats. The National Highway System is a key component of national defense mobility. It is the key link for the military to railroads, seaports and airports for personnel and supplies. The Strategic Highway Network supports the mobilization of the Armed Forces as required.

IMPORTANCE OF RECOVERY AND MITIGATION FOR A TMC

One of the prime factors that effect the required investment in recovery and mitigation plans is the timeframe that the community may be without the services provided by the TMC. Allowable timeframes for systems outages are often difficult to determine. The timeframe should be based on both normal functions of the TMC and functions of the

Allowable timeframes for systems outages are often difficult to determine.

TMC during community-wide disasters. Allowable timeframes may also be different due to the day of week, time of day, or specific events that are occurring. Planning must take into account the worst case scenario where given all of the possible situations, the least amount of time that the community may be without these services.

It should be remembered that it is possible and even likely, that various TMC functions have different required availabilities. Some functions may be needed within several hours, where other functions can be unavailable during emergency situations for days, weeks or even months.

Within this analysis resides the second prime factor that effects the required investment in recovery and mitigation which is the integrity of previously stored data (i.e., the currency of the data that is available to the system upon being restored). In the case that data updated or stored by the system, such as log files, must be accurate and available up to the second that the system became unavailable, the methodology for recovery and mitigation will be far different than where the system updates and logs can feasibly be deleted for days without any negative repercussions. Requirements of specific functions and the preservation of previously generated data will drive the methods of recovering the TMC.

Regaining normal operations is a topic that is easily overlooked. The obvious beginning point for restoration of normal operations is the elimination of the problems that caused the need to be in a recovery mode. But, regaining normal operations must be planned and implemented in much the same manner as the execution of recovery procedures was planned and performed. During the restoration process, many of the same concepts are at work including the speed and timing of the switch as well as the integrity of the stored data. Complicating the restoration is that the support staff is likely to already be involved in restoring other departments and relative priorities must be taken into account.

Types of Mitigation

An often quoted truism is that the best way to handle a recovery situation is not to have one. Mitigations of circumstances that could result in recovery should be a primary focus of TMC management. As is true when considering recovery, in planning a mitigation strategy TMC management must assess the cost/benefit of individual types of mitigation including, but not necessarily limited to physical infrastructure, cyber infrastructure, loss of personnel, and community-wide disasters.

The physical infrastructure that should be considered is the building and all of the utilities that are required to respond to possible circumstances may include preventing the incident from happening such as fire suppression equipment to limiting the exposure if/when the incident occurs such as through the use of UPS and power generators for loss of power. Redundancy of individual infrastructure elements is also a valid mitigation strategy. Receiving power from multiple substations and telephone lines from multiple central offices are examples of this type of redundancy.

Cyber intrusion is quickly becoming one of the largest risk areas for the nation's critical infrastructure. This type of attack may be launched locally, or just as easily it may be launched from across the county or from across the world. The most common risk is that of data security, that is knowingly or unknowingly giving access to data and functions to those that should not have the access. In the area of data security, a significant risk comes from errors that are made by trusted, well-meaning employees. Much of the mitigation for data security is to institute and follow stan-

standard data security policies. Data security policies include how access is granted, when it is taken away, and the use of the TMC network for non-work.

Viruses are a well known threat which comes in a variety of forms. The news media is constantly reporting new viruses that have begun circulating and reeking havoc on organizations throughout your community and the country. The standard mitigation for viruses includes standard technology policies that are followed by all personnel as well as the installation and continuous updating of virus protection software.

Service interruptions may be caused by the loss of specific skills and knowledge that only specific people possess. A mitigation strategy for this type of risk may include training backup personnel in all jobs as well as documenting all job functions within the organization. This is not to say that an organization will always be able to function at 100% given the loss of one or several individuals. More, these types of mitigation will provide a method of rebounding from a loss of this type.

Mitigating community-wide disasters involves:

- u Alternate Sites
- u Documentation
- u Testing

Alternate Sites

A high end, costly recovery solution that may be thought of as an ultimate mitigation strategy is that of having a fully redundant TMC. By utilizing this type of site on a stand-by basis or for overflow work, procedures may be put into place to allow for no interruption in services being rendered due to an emergency situation having occurred. This is the most costly approach to recovery, but also may be viewed as the ultimate mitigation. Depending upon the specific configuration and procedures, a redundant site could provide for no down-time and no loss of data during transition. It should be remembered that, if the primary and redundant site are in close physical proximity, they may both be adversely affected by an event.

Alternate sites may be able to provide redundant infrastructure and TMC capabilities at a lower cost. As has been suggested earlier, the effect of this lower cost tradeoff is a longer time to restore the services. Alternate sites may include hot sites, cold sites, trailer sites, or cooperative backup agreements. Each of these types of alternate sites has their own complexities and issues.

A hot site is a TMC that stands ready to be set up as the operations environment for an organization. These frequently consist of a commercial subscription service that would be used by multiple organizations. Use is allocated for recoveries on a first-come, first-serve basis. If the preferred hot site is already in use, another site is made available. The alternate site may be farther away from the community that may be desired. There is always a possibility that all of the hot sites are in use at any point in time. Subscription fees normally include this type of availability and periodic testing. Actual use of these sites is normally charged separately.

Cold sites are buildings that include infrastructure items with long lead times to install, but no specific computer equipment. A cold site would typically include a PBX, wiring, HVAC and raised floors. It is the responsibility of the occupying organization to furnish all other materials to

make the cold site operational. Cold sites would normally be used as a longer-term solution than a hot site after the initial hot site usage has been completed.

Trailer Sites may be leased as either hot or cold sites in that they may or may not include the actual computer equipment. The trailers are then moved into an appropriate position for use in operations.

Cooperative Backup Agreements are agreements that have been made with either other agencies within your municipalities or other TMCs in outside of your municipalities for use of their operation center in case of a system stoppage. In establishing such an agreement, this usually means that the agreement is reciprocal. As will be discussed later, one major issue with an agreement of this type is that allocation for space and equipment is kept to the minimum resources required for the organization to fulfill its goals. Extra resources are not made available thus; the use of the operations center by another organization will not be possible.

Documentation

Documentation is key to both recovery and mitigation strategies. By fully documenting processes and procedures, those other than the key staff members could be used to run the TMC to mitigate an emergency situation if necessary. Documentation is also imperative to efficiently and effectively recovering the TMC at an alternate location.

Creation of documentation is the beginning, not the end of the preparation. Once created, documentation must be kept current. Including processes of updating documentation during every system change project as well as periodically reviewing and updating documentation to ensure accuracy is vital. Availability of the documentation is a final piece that makes the documentation usable. Having the documentation available to appropriate staff members when needed during an emergency situation will aid in rectifying the problems that occur.

Testing

Testing will help to validate that the documentation is accurate and up-to-date. In periodic testing, identifying errors, and updating documentation appropriately, the documentation should be usable in the case of a system stoppage.

Periodic and ongoing testing is vital to any recovery effort. Different types of testing may be accomplished including desk or scenario testing and test activation of alternate sites. Testing is able to point out deficiencies in the recovery plan. Successful tests are not those that are completed with no errors, rather those that point out updates that are needed to the plan. Testing may be scheduled and planned or may be accomplished with no prior warning. The ultimate test of recovery capabilities is to have the recovery performed by people that are trained in the base knowledge but do not work on the particular system. In this way the test validates both the plan and the documentation. It provides for the ultimate recovery possibilities for the TMC.

¹ InfoTech Research Group, *Building a Comprehensive Disaster Recovery Plan*, 2005

² http://www.cert.org/stats/cert_stats.html#incidents

³ Warrick, Cathy, et al, *IBM TotalStorage Business Continuity Solution Guide*, International Business Machines Corporation, 2005, ISBN 0738491136, Page 25

2

SYNTHESIS OF CURRENT PRACTICES

Chapter 2 Purpose:

To review the state-of-the-art of recovery and mitigation (aka, contingency planning) in the industry and the state-of-the-practice as found within TMCs. Best practices that have been found within TMCs will be reviewed in order to present an understanding of processes and procedures that may be applicable to individual TMCs.

Chapter 2 Key Message:

- u State-of-the-art concepts of Recovery and Mitigation, also known as contingency planning
- u State-of-the-practice concepts Recovery and Mitigation as it is practiced in TMCs
- u TMC best practices as related to Recovery and Mitigation

STATE-OF-THE-ART

Organizations that may be thought of as having a state-of-the-art environment in recovery and mitigation possess a true management knowledge of and commitment towards recovery and redundancy. Policies within these organizations have been established so that recovery and redundancy is taken into account in all phases of the business. These organizations consider planning for recovery and mitigation an important element of the planning process. Ongoing testing is an important factor within these environments to validate the plan. Part of the reason for ongoing testing is to test the documentation. Complete and current documentation is key to organizations that possess a state-of-the-art recovery and mitigation environment as is a considered approach towards planning alternate sites that may be used for the operations.

Management's Commitment

Management in the state-of-the-art recovery and mitigation environment consider this topic a priority. This priority extends to the point of considering recovery and mitigation when thinking about all changes to the environment. Management sets up processes and procedures that require changes to pass through an analysis of the effects of the change on the existing recovery and mitigation plan. This may be accomplished through the use of periodic meetings that review all changes, having to document any expected effect and the related methods of handling these effects or having a specialist in recovery and mitigation review the change with an eye towards possible effects.

Budgeting in state-of-the-art recovery and mitigation organizations includes continued allocations for upgrading the plan. As changes occur within the organization as well as interfaces with other organization, the plan must be revisited and revised to take the changes into account. Ongoing testing of the recovery and mitigation plan will find errors and the necessity for changes

that have not otherwise been found. Funding for this continuous work should be included in the annual budgeting for state-of-the-art recovery and mitigation organizations.

In order to optimize the use of the scarce budget that is typically available for recovery and mitigation while still ensuring that appropriate risks are addressed, appropriate policies must be established. Policies, by their very nature restrict creativity in the development of new processes. Policies should be used when necessary in order to ensure that communications of critical requirements are made and codified for those putting together new processes.

Policy Issues

An important initial policy to consider is the establishment of an executive sponsor. A champion for recovery and mitigation is of ongoing importance in order to ensure that the correct level of priority is given to this issue. Many organizations assign this responsibility to the senior technology manager because traditionally, a large part of the plan has been focused around the organization's technology platform. The issue of whether to give this position to a technology manager should be based on both the position that this manager holds in the organization and the respect that this manager is given by other managers at all levels. The project champion must be at a high enough position that they can ensure that recovery and mitigation will be factored into all work that is being done by the organization.

It should be noted that two months following the 9/11 attack, 53% of the senior technology officers of major organizations stated that their organization had continuity plans and less than 50% had security training programs for staff.⁴ The largest organizations within the United States had not accomplished this important task at that point, even with senior management understanding the need.

Standardization of hardware and software that is used in an organization has the potential effect of lowering the total cost of ownership for technology within the organization. From a recovery and mitigation perspective, standardization of this type will allow for a more efficient and effective mitigation strategy as well as a more expedient recovery scenario. The requirement for standardized hardware and software should therefore be considered as a policy to be developed.

Management should also establish policies on the proper handling of data including availability, confidentiality, and integrity. In order to properly handle data, considerations should be given to backups, document management and security. Policies relating to appropriate backups must encompass both system backups and backups of personal computers. Care must be given to providing for backups of data residing on any laptops that are being used. Once the backups are completed, the data must be stored in a different location than that of the original data. The location and labeling must be standardized so that the proper backups may be easily accessed when needed. As will be discussed later, an option is to have all backups stored on servers used specifically for backups using the internet. These servers may reside anywhere in the world, and would have security in place to ensure that unauthorized people could not access the data.

In order to utilize backups, it is critical to require testing through use of periodic restores. Backup data stored off-site is of no use without the ability to restore it to the original system.

Document management relates to storage of official documents for the time required by law. These documents may include logs of the actual functioning of systems within the TMC. It should be remembered that both the length of time that a document is to be saved and the assur-

ance that after that time the document will be completely destroyed is required for any well run organization. The relationship between document management and recovery and mitigation is based on the timing and types of backups which are to be stored.

Security standards must be set as a policy by management to provide for an important mitigation factor. As will be discussed in chapter 3, security includes providing for use of up-to-date virus protection, allowable access by employee level, use of the internet and email, turning off access privileges upon termination, physical access to critical areas of the TMC and physical access after termination. Setting and enforcing security policies is a prime form of mitigation for state-of-the-art organizations.

Organizations that understand the importance of recovery and mitigation have clear policies communicated to all staff members defining personal responsibilities during times of outage in the operations center. In order to quickly restore critical systems within an operations center staff must be available without consideration to time-of-day or day-of-week. Emergency operations of this type may require some combination of relocation and long hours of work.

An exact definition of what constitutes a recovery situation is codified as a policy by state-of-the-art organizations. In thinking through the complexities of recovery and mitigation, most thought is given to how to mitigate outages and how to recover from an outage, both of which are very important. But, equally as important an approach to defining an outage situation that must be recovered is necessary. Systems, large and small fail periodically. Emergency procedures should not be put into effect for each outage. A policy should be codified that takes into account requirements for the system availability and complexities of each individual system. By codifying a policy of this type in advance, at the point that an outage occurs the decisions do not have to be thought through from scratch.

Lines of authority during emergency system outage situations are codified in advance through the use of policies in state-of-the-art organizations. The physical location of the operation may change during these periods of time. Specific staff members may not be available during these situations. Creating a policy that specifies the lines of authority is imperative for the smooth running of an operation during emergency situations.

Organizations that make a true commitment to recovery and mitigation codify interdepartmental communications needs, methods and authority within policy. At times of system outage it is imperative that appropriate staff members of other departments within the organization are notified. They must be notified with accurate information at the appropriate time. In thinking through these needs, appropriate staff functions are identified as the focal point for communications. Identification of who is to be communicated with and the appropriate timing of the communications is also codified.

External communications during an emergency situation may be one of the most serious tasks to be undertaken. Organizations that are well prepared and organized for emergency situations think through all external communications paths and prepare communications plans before an emergency takes place. Included in a communications plan and policy is identification of the staff member that will be the external contact for each particular type of communications. A different person may be selected to speak to the media than is selected to speak to outside organizations. The tone, message and specific information should be consistent. Appropriate communications aids in keeping the community calm in the face of the emergency.

Planning

Planning is the critical initial step for the state-of-the-art recovery and mitigation organization. Appropriate planning ensures that the work being accomplished has allocated the correct amount of resources for both the planning and the execution of the plan. It should be remembered in the planning process that systems are made up of hardware, software, people, facilities and procedures. When an agency is planning for recovery and mitigation, all of these components must be taken into account.

When establishing the appropriate level of recovery and mitigation, the organization begins by determining their mission. The mission specifies the purpose of the organization; what the organization is about, what it is not about; what the organization will achieve and associated metrics; the scope of operations and their relative priorities. By determining the mission, the requirements for recovery and mitigation may be determined and an appropriate level of planning and ongoing execution resources may be allocated.

After determining the mission of the organization, relative priorities are assigned. Resolution of priorities needed within the recovery and mitigation project, as well as between this project and other development projects currently underway should be made. Any prioritization exercise is a trade-off of competing factors. This is no exception to that rule. There is a limited budget, limited staffing, and a limited number of hours in a day. There are many times easy solutions and hard solutions. Which is picked and the priority given will be a function of the organizational mission and the executive sponsor.

Budgeting for support of recovery and mitigation versus a project to improve productivity or provide new services is a tough call for any organization. Creating metrics for recovery and mitigation as an organizational goal helps to moderate this challenge. Examples of metrics that may be used include number of errors found during testing and time test takes to restore the TMC at the recovery site.

Relative prioritization also becomes an issue relative to the processing window. The time that is available in which to perform backups is limited. Limitations are due to the hours in which staff is available and the hours in which system availability is required. An example of the tradeoffs that must be made is that there are a fixed number of hours that staff is available to perform backups, and there are a fixed number of hours that the system is required to be available. When the system is required 24 hours per day, 7 days per week, there is no availability to back up files that are being utilized by the system. If the system is not needed all hours, but during those hours staffing is not available, again, there is a resource constraint. There are various methods of solving this constraint issue. Each of them requires the expenditure of resources. You may staff personnel for additional hours, or redesign the system so that the files may be backed up while the system is running, or you may keep mirrored copies of the data base where multiple copies of the files are updated at the same time. Another alternative may be not to do backups if you have no requirement to save data that is being processed. Again, this goes back to the overall mission.

In addition to determining the relative prioritization of recovery and mitigation, organizations determine allowable downtime from the mission and related requirements. One of the primary factors that determine the cost of a recovery and mitigation program is the allowable downtime. How much downtime is acceptable? That depends upon the mission of the organization. It also depends upon the functionality that is required during normal operations and the functionality required during emergency operations. The amount of allowable downtime will also have an ef-

fect on the policy, discussed above, as to the process for declaring an emergency situation. The shorter the allowable downtime, the more direct process will also be needed.

As an example of increased cost for shorter allowable downtime, the following is an extension to the backup example discussed above; there are various solutions that might be used to backup an operational environment. Some examples which provide from low to high availability are:

- u Tape Backup
- u RAID
- u Electronic Vaulting or Remote Journaling
- u Load Balancing or Disk Replication
- u Virtualization

Each of these presents a different method to backing up data. As one moves from low to high availability, the cost increases correspondingly.

The second primary factor in determining the cost of recovery and mitigation is the determination of the allowable integrity of data. In this context, integrity of data is defined as the currency and correctness of data at the time of system restoration. By this definition, the highest data integrity is when the data is available at the time that the system is restored and that data is accurate until the moment that the system stopped. The other end of the spectrum is that when the system is restored it comes up without data other than those parameters needed for it to execute properly as it did when initially installed.

Data bases may be sub-classified as data, log files, and archived log files. In fully understanding the mission and requirements of the organization, a decision can be made as to the need for and frequency of backups. In some systems the data are transactions that update files. In other systems, this data does not change anything dynamically; rather the data is initially set up at installation or upgrade and is static after that point. Data in this context is the parameters and information that is used by the system in order to run correctly. When this is true, data need only be backed up upon installation or upgrade. In this case there is no reason to perform these backups on a daily basis.

Log files are those that keep a copy of all information that has flowed through the system. They may be used in order to recreate actions that have happened or to analyze the flow of data received. The need for these file will span the gamut of not needed but it has always been available to an organization that may not meet its mission without all data being available. The amount of time for which this data may be lost without serious impact will dictate the type and related costs of the backups.

In order to keep log files to manageable sizes, older data is deleted from log files and may be saved as archived log files. As is true in the log file example above, the necessity of these log files to the mission of the organization may be significant or may be minimal. It should also be understood that at predetermined intervals the log files should be deleted as was discussed in the policy section.

By determining the requirement for integrity of each type of data the appropriate level of backups may be determined. With this information, the organization then allocates the level of resources necessary to satisfy the organizational requirements.

Once the two primary requirements of allowable downtime and data integrity have been defined and agreed to, the actual planning for recovery and mitigation may begin. The planning project for recovery and mitigation is much like any other project and follows the same basic structure that each organization uses internally. Organization specific project management tasks often include approvals, budgeting, status reporting and the like. Other than these types of tasks, a recovery and mitigation project has a set of tasks that should be accomplished in any organization. A typical project as outlined by IBM⁵ consists of the following tasks.

Project Initiation and Team Selection. In this initial task of the project, all organizational approvals are granted. All forms and methods of collecting the needed information are standardized so that each team member can more easily proceed with their tasks. All needed resources are allocated, including the identifying and scheduling of all team members.

Data Collection and Critical Needs. All information about the flow of data within the organization is collected. Information is also gathered pertaining to the technological infrastructure, the risk of system outages and related costs. Any known mitigations to these risks are also gathered at this point.

Risk Analysis. This phase is the analysis of the information gathered during the Data Collection and Critical Needs phase, above. In this phase, an understanding is gained as to the organizational risks of systems outages and the associated costs of recovering within the acceptable time frames. Mitigation technologies are able to be justified through these analyses.

Data Protection. A separate analysis is performed to address the physical and logical protection of data. This analysis may conclude in additional policies or procedures being developed, or the addition of physical security devices. In many cases these steps are mitigation measures.

Recovery Plan. As in many projects, there is one task that at first glance is thought of as the only task necessary. In this project, this is that task. Using the information that has previously been gathered, an approach is determined and documented for replacing systems, networks, and staff members due to a severe system outage.

Training and Testing. After the plan has been completed, the training and testing task will validate its accuracy and point out places for improvement. It will also give the team needed information on how to proceed in case of a system outage. This task is an ongoing one and should be repeated several times per year in order to keep the staff educated and to validate that changes in the environment do not adversely impact the plan.

Change Management. This is also an ongoing task. As the environment changes within the organization, change management should be used to ensure that the plan is kept up to date.

During every major disaster that has occurred, communications ranks high on the list of important issues. The National Institute for Science and Technology's Contingency Planning Guide for Information Technology Systems⁶ reminds us that plans should account for the possibility of the operations center being a "communications-forwarding point between personnel, civil and federal authorities, and affected families and friends" during times of significant disaster.

With the communications infrastructure that resides within the country, it is also important for any recovery and mitigation plan to recognize and take into account that staff members may have the ability to work from their homes or from wherever they are residing given an internet connection. The plan should use these capabilities if appropriate.

Testing

Testing is meant to validate and note possible improvements to the plan once completed in order to ensure that it meets the organizational requirements. With the complexity that resides within the systems of all operations centers, testing the plan is fundamental to ensure that it provides the expected results.

Changes to either the operations center or other entities that interface with the operations center may require changes to the plan that had not been anticipated. Ongoing testing of the plan will bring these necessary changes to light. Changes as insignificant as an adjoining municipality requiring area code to be dialed with the phone number can create an error within the plan that must be corrected and distributed.

In order to keep the plan up to date and accurate, full testing should be accomplished at least twice per year. Desktop testing, also known as scenario testing, should also be completed twice per year. By performing these tests, the staff is able to review the plan closely and take notes on both errors and possible improvements. Identified improvements also have the possibility of improving the fundamental organizational processes as well.

Desk testing should be performed periodically where a group of senior operations staff can spend a day logically walking through different scenarios of systems stoppages in order to find holes in the current plan and possibly operational processes. In developing scenarios that could occur, the team may discuss the procedures that will be put into place for determining if an emergency exists and how the situation would be handled. Scenarios may include such events as fire, loss of communications lines, job actions, flood, epidemic, and hard disk crashes.

In the case of desk testing the objective is to find errors in the logical makeup of the processes. By thinking through various scenarios, the team has the opportunity to find gaps in the processes that may be filled.

Recovery testing is that which would be held at the alternate site that had been picked to back-up the operations center. In this testing, the team progresses as if the operations center had been lost. Communications infrastructure, operating systems, applications and data are installed. Installation is completed for both servers and workstations. Tests are then run to validate that they system is still working as expected.

The objective of recovery testing is to test both the process and the tools that are being used. Actually establishing communications and using backups to restore servers and desktops allow the testers to find errors in the recovery process that may be corrected before the plan is to be used.

A staff member should be present to act in an audit role during all testing. This person should take notes that specify all errors encountered. After the testing is completed the auditor should prepare a report of all errors during the test. These should be the input to additional tasks to be completed in order to upgrade the plan. These items should be reviewed before the next test to ensure that they have been rectified, and tested for specifically on the following test.

Documentation

The main tangible deliverable from a recovery and mitigation project is the documentation. In any operation center, the amount of documentation that is necessary is significant. Specific organization of the documentation varies from installation to installation, but the following list is an example of the types of documentation that is present in a state-of-the-art environment.

- u Contingency Plan
- u Network Documentation
- u System Passwords
- u Personnel Contact List
- u Process Manual
- u Procedures Manual
- u Policy Manual

In addition to this list, all of which are considered recovery and mitigation documentation, another important document exists outside of that realm that should be within the organization -- an Occupant Emergency Plan (OEP). This plan is normally part of personnel planning used for day-to-day operations, but it is important that it be kept up to date. It is a plan which outlines the exit procedures during an emergency situation. It includes methods for exiting the building and collecting headcounts of staff members. The OEP is normally tested during periodic fire drill exercises.

The primary documentation is the Contingency Plan. This plan contains step-by-step instructions for all actions to be taken during an emergency situation. It begins with the decision making process for declaring an emergency situation. Mobilization of, and logistics for the emergency team and all materials needed at the alternation site are also included. Restoration and validation instructions are also included within this documentation. In addition to the items listed below, some, or all of the other documentation may be included in the Contingency Plan. Where appropriate, references to other documentation should be included in order to document specific information one time only. When a reference to other documentation is included, copies of the referenced documents should be stored with the Contingency Plan.

A significant portion of restoration of services is based on restoration of the underlying network infrastructure. An important component of a plan is a fully documented, current network layout. This will provide information for the personnel that are reconstructing the operations center to use as a basis of the reconstruction. This may be included as a part of the Contingency Plan or may be a separate document that is referred to within the plan.

Documentation of all system passwords should be kept separately from all other documentation. Separation is due to the risk of these passwords being released inappropriately. The Contingency Plan may be distributed to each team member and selected management personnel. Passwords should be restricted on a need to know basis. This is true even during an emergency situation.

Contact lists are important during any system stoppage situation. The lists should include internal staff members, external contacts, and vendors. To be valuable, the lists must contain all contact information for both during normal business hours and off-hours including nights, weekends and holidays. Home and work telephone numbers, cell phone telephone numbers, beeper numbers and EMAIL addresses should be maintained where appropriate. In the case of external contacts and vendors, primary and backup contacts should be maintained. As was true with the systems passwords, it is normally appropriate to keep these lists confidential and have them distributed on a need-to-have basis only because some of this contact information may be considered confidential.

Standard documentation used during the workday should be part of the documentation that is available during an emergency situation. Documentation should include Process, Procedures and Policy Manuals. These manuals may be referenced in other documentation, but more important these documents are likely to be needed during daily operations at alternate locations.

Appropriately storing the documentation is vital to being able to use it in case of an emergency situation. The documentation must be stored off-site in order to be able to be accessed if the operations center is inaccessible. At least one set of the documentation should be printed so that it may be used before the computer systems are available. Additional copies may be available in softcopy format. These may reside in various places which may be accessed from outside of the operations center. All copies should be secured with only those with a need to know gaining access to them. Even copies of the documentation that do not contain passwords and contact lists are organization confidential. They contain significant information that should not be publicly known.

If copies of the documentation, in whole or in part, are distributed, they should be subject to rigorous configuration management principles. Each document should be numbered and signed out to a specific person. In this way, the copies may be retrieved if the person leaves the organization. Configuration managed copies are also easier to keep up-to-date as required changes are published.

Alternate Site

At a time where the primary site of the operations center becomes unusable for various reasons, an alternate site should be used which has been previously identified and for which plans have been documented. Various types of alternate sites are being used today. Each provides different features and relative costs. The alternate site possibilities in order from the costliest to the least costly are redundant site, hot site, cold site, and cooperative agreement. There are also derivatives of each.

A redundant site is having a second operations center that always stands ready with the hardware, software and communications infrastructure already in place and running. This backup site may take over operations at any point needed with no specific start-up to execute. In fact, with a second site of this type available, part of the operations may always be run from the second site and the only difference that would occur during a system outage would be that all staff would work from the one operations center rather than being spread over two different installations. This is the fastest mode of recovery and normally the most expensive. The other issue with a redundant site is that it normally resides close to the main operations center. If the emergency is a community-wide emergency, both the primary and redundant sites may become inoperable.

A hot site is an operations center that is set up with all the needed hardware and network infrastructure, but without your software running. Hot sites are normally shared by several different organizations and specific ones are available on a first-come first-serve basis. If a community-wide emergency occurs, it is possible that the hot site may not be available. You may be moved to an alternate site in a different area, far away, or possibly have none available that will meet your needs. If open, the hot site is immediately available to your organization upon declaring the emergency. At that point the site must be restored with your organization's software. Hot sites are normally subscription services where an annual fee is paid providing for testing time and the ability to use a site if needed. Use of the site for an emergency is frequently at an additional cost.

Cold sites provide the infrastructure of a building, some wiring, HVAC and PBX. The rooms may then be quickly filled by your organization with hardware to run your operations. Setting up operations in a cold site will take longer than either redundant site or hot site, but is less costly. Depending upon your exact requirements the cold site may be able to be delivered to a location of your choosing as a trailer, or may be a constructed building that you move into. Many times a cold site is used after time has been initially spent in a hot site.

The least costly alternative is a cooperative agreement. With a cooperative agreement it is common to make a reciprocal accord with either another agency in your municipality or an equivalent agency in an adjoining municipality. These agreements frequently have little or no cost associated for rental of the space. But, given that, there are several issues associated with the use of cooperative agreements. Most of the issues revolve around a simple fact that is common to every operations manager in every organization -- they are asked to work with as few resources as possible while maintaining a high level of service to their customers. It is uncommon that operations centers would have enough extra equipment and space to enable an influx of all of the personnel and work from another operations center which may last for a considerable amount of time. Also unlikely is the ability to periodically take space from an existing operation in order to test a Contingency Plan.

No matter what type of alternate site is chosen, several basic issues must be kept in mind:

All software licenses must allow for running the system at an alternate location for either tests of emergency situations or for true emergencies

Any backup files that exist must also be able to be easily and quickly transported or communicated to the alternate site

Communications lines that normally terminate in an operations center must be able to be rerouted to the alternate center

STATE-OF-THE-PRACTICE

The current state-of-the-practice of recovery and mitigation in TMCs covers a wide spectrum from "...what is recovery and mitigation?" to "having an immediate switchover to redundant sites and every system component being redundant." The differences between each end of the spectrum as well as gradations in between the two extremes are a function of many individual issues including knowledge of recovery and mitigation, relative prioritization and management commitment.

Management Commitment

By and large; the TMCs that have progressed in their efforts towards recovery and mitigation have also reported management support and commitment for the effort. There are numerous reasons driving the commitment, but the commitment is a constant. Drivers have included media awareness of the issues, previous encounters within their organization of severe systems stoppage and knowledge of occurrences within other organizations.

The executive champion of recovery and mitigation within the TMC organization is normally a high level individual that is focused on the problem. They have the knowledge that if a significant outage occurs, there could be significant impact on the municipality. Because of this, the

executive considers recovery and mitigation to be a fundamental organizational decision and priority. Recovery and mitigation is to be considered as a portion of all decisions that are made.

TMCs that are committed to recovery and mitigation provide senior level resources to think through recovery and mitigation issues, thus striving for continuous improvement in the organization's capabilities. Some TMCs go to the extent of having weekly status meetings attended by all senior operations managers to discuss the current and future recovery and mitigation efforts. These meetings provide the staff a visible indication of senior management's commitment to being prepared in case of a systems outage.

Funding for initial and ongoing development and testing is included in every year's budget. In most cases rather than having direct line-items for recovery and mitigation, there are policies and procedures that ensure that every project undertaken within the TMC include funding for any recovery and mitigation implications.

Policy Issues

Many TMCs have instituted policies that support recovery and mitigation within the planning, testing and execution stages. The policies require senior management approval and buy-in, again showing management commitment to the process and final outcome.

Policies that have been enacted to help mitigate the risk of systems stoppage include those directed towards staff of the TMC and those directed towards the design and implementation of the technology infrastructure. These policies are meant to either reduce the probability of an outage occurring or to lessen the impact of a system outage if it does occur.

Fundamentally, a set of policies is used to restrict physical and logical access to only those that require that access. Often staff members are given access to everything to cut down on the complexity of the security system, or because each staff member believes that they deserve this access. The policies extend to the requirements involving cancelling both physical and logical access immediately upon leaving the organization.

Restricting access of individuals allows the obvious advantage of not allowing embittered employees' access to make unauthorized changes. Of more importance is that restricting the security of employees prevents mistakes being made on the system by those that are not fully trained. The biggest security risk in the opinion of most data security managers is that of an employee making a mistake on the system.

Mitigation focused policies include both those to mitigate the risk of having a system outage and those that mitigate risk during the recovery process. Some risk mitigations actually fit into both categories.

Complexity of the systems infrastructure by its very nature imposes additional risk. Complexity is being reduced through policy by mandating such things as

- u Standard workstations operating system and hardware
- u Standard servers operating system and hardware
- u Standard office automation products
- u Standard project management tools
- u Standard telephony equipment

- u Standard TMC applications
- u Standard data storage

Risk mitigation during the recovery process may be assisted by policies that express management's desire to fundamentally assure that minimum acceptable standards are followed. These policies include:

- u Method of performing backups
- u Schedule of performing backups
- u Storage of backups
- u Access to backups during a recovery situation
- u Access to documentation during a recovery situation
- u Personnel activation during recovery situations

Several decisions may be made prior to a recovery situation and codified as a policy in order to eliminate as much decision making as possible during a situation of this type. Policies of this type will aid in providing the staff with a workable environment in which to work during a system outage.

- u Clarify who may activate certain emergency plans
- u Restrictions on procurement authority loosened
- u Integration of TMC with the emergency management office for community-wide conditions which includes complete information sharing
- u Established protocols for communications between TMC, law enforcement, fire and rescue, EMS and emergency management officials
- u Communications with the public using the media and advanced traveler information systems.

Planning

TMCs that have experienced considerable systems outages use a basic premise of planning to expect the unexpected. They have already experienced that a series of events that, if it were brought up as a possible scenario, would have been dismissed as being impossible. An example of this was the Northeast Blackout, Great Lakes region in which the scenario was described by the Federal Highway Administration in a May 2004 report:⁷

Shortly after 2:00 p.m. on the afternoon of August 14, a brush fire caused a transmission line south of Columbus, Ohio, to go out of service. This was followed at 3:05 p.m. by the failure of a transmission line connecting eastern and northern Ohio, which was in turn followed at 3:32 p.m. by the failure – caused by a sudden excess of power flow – of a second line in the same area of northern Ohio. As more and more portions of the electrical network disconnected from the grid, the events on August 14 quickly accelerated: five transmission lines between Ohio and Michigan failed within the 30 minutes between 3:30 p.m. and 4:00 p.m. At 4:10 p.m., the electrical system connecting the region south of the Great Lakes, including the cities of Cleveland and Detroit, to New York and New

Jersey experienced a profound failure...Within a single minute, many transmission lines failed throughout the entire area, creating a cascading effect in which lines sequentially overloaded and then failed, leaving a swath of 3,700 miles – including portions of Vermont, Massachusetts, Connecticut, New York, New Jersey, Pennsylvania, Ohio, and Michigan, up through portions of the Maritime provinces – in the dark. On one August afternoon, a series of seemingly small events, happening in concert, produced the largest blackout in American history.

This progression of events was not expected. The effects were much wider spread than anyone would have anticipated which is true with many community-wide disasters. The goal of planning in TMCs that value recovery and mitigation is to plan and expect the unexpected.

These TMCs realize that the extent of planning and preparation must be based on overall organizational goals. As discussed previously, an analysis of the goals and objectives for the TMC is the underpinning of a recovery and mitigation plan. Following this, requirements for recovery and mitigation are developed. No two TMCs will have matching goals, objectives or requirements. As such, this means that no two TMCs will have identical recovery and mitigation plans.

During periods of operational recovery and mitigation, most TMCs have found that significant problems exist with communications. State-of-the-communications-practice for TMCs includes use of multiple communications paths which avoid systems outages. By maintaining multiple communications paths, the TMC is able to avoid a systems outage based on a single communications outage from a single central office or an individual line. There is also the possibility of providing multiple fashions of data communications infrastructures such as wireless, DSL, broadband and dial-up connections.

TMCs that fully consider the complexities of systems outages that are combined with communications outages have established alternate forms of voice communications. These include supplying staff members with cellular phones and equipping the TMC with telephones that do not require electric connectivity for their operations. Staff members carrying cellular phones may qualify to have their cellular telephone accounts pre-approved with Wireless Priority Service (WPS) which will allow priority for cell phone calls once activated for individual calls. This service, which is administered by the Department of Homeland Security, may be activated during periods of emergency within an area.

Due to the loss of regularly used TMC-to-public communications, some forward thinking TMCs have identified alternate forms of communications that may be used. An example of this is the budgeting for the purchase of media spots that may be used during periods of emergency conditions. The spots may be used to notify the public of the exact, un-interpreted message necessary for communications with the public.

During periods of emergency, even if the TMC does not lose communications lines, it is likely that telephone calls will be unable to be completed. People calling into the area from other locations to check on the status and welfare of the area will fill the circuits, not allowing important calls to be made. The TMC may register for the Government Emergency Telecommunications System (GETS) which will allow the TMC to have priority in their voice calling during these emergencies.

Another provision made by TMCs is having voice telephones that do not require electricity for operations. These telephones will allow for the use of voice telephones when no electricity is

available. Often called POTS (plain old telephones), technology that is not up to state-of-the-art will often allow meeting fundamental goals.

Mitigation of power problems is normally through the use of multiple power feeds from various substations and/or various grids. Each additional feed substantially reduces the possibility of experiencing a power outage. Even with significant mitigation steps in place, the Detroit-Windsor Tunnel's use of four separate power feeds did not prevent a power outage during the Great Lakes Blackout.⁸

In the case where all power interruption mitigations fail, emergency power can be supplied by Uninterruptible Power Supplies (UPS) and generators. UPS systems supply power for a short period of time, holding the power until generators are able to start. Various TMCs have reported that they have identified the minimum equipment that is necessary to maintain their operations. These are the ones that are supplied the emergency power during these periods of time.

When long power outages occur, fuel tanks may need to be refilled while keeping the generators running. Refilling fuel tanks in this way is an activity that presents additional risk. It should be planned for and tested before a power outage occurs.

During times of systems outages, roadway instrumentation may also be adversely effected. Power fluctuations, voice and data line losses, high winds, severe flooding and the like will have negative effects on instrumentation that resides on the roadways. If the TMC is able to keep their utilities active, this does not assure the roadside instrumentation availability. CCTVs, DMSs, signals and other instrumentation needed to understand the state of the community and allow vehicles to leave (and possibly enter) the affected area may not be available. Some TMCs have determined that in addition to planning and equipping for alternate utilities within the TMC they must also perform the same type of planning for roadway equipment.

Recovery and mitigation techniques that are used in TMCs allow the staff to have command and control of the field devices on the roadway. They are able to monitor activities as well as use the equipment to assist in mobility and communications. These functions are valuable to others to assist in response to the emergency. TMCs have reported sharing the data and TMC facilities with local emergency responders, federal emergency responders, and even the transit departments to assist in meeting community needs.

Contacts and relationships with other agencies are made during planning sessions. Planning sessions are often a function of the emergency response offices of the municipalities which are attended by the TMC staff. The contacts are specific including contact methods for both normal business hours and off-hours. In the planning meetings, lines of demarcation of responsibilities should be agreed upon. Communications paths should also be documented, as should any related protocols.

Truly prepared TMCs provide continuous staff training on recovery and mitigation. The training, when working in an interagency environment includes staff members from each of the agencies. The training is used to encourage staff members' support of the effort as well as understand the interrelationships. Training normally includes testing with other agencies in a group effort. Interagency testing provides camaraderie between agency personnel, ability to find errors in interagency coordination, and a good testing environment.

Testing

Ongoing testing provides a number of important benefits to the TMC. The obvious benefit of initial and continued validation of the TMCs recovery and mitigation efforts, in and of itself is important. By testing as an ongoing function, the TMC is able to understand the effects that changes to the TMC and external interfaces have to the recovery and mitigation plan.

During initial planning efforts, TMCs have found energy to move forward and complete the task. The forward movement can easily end after the initial planning project is complete. Pre-scheduling future tests every x months gives the project continued visibility and importance. This helps encourage and remind staff members to think about recovery and mitigation in the development of all projects undertaken.

Testing identifies both problems with the plan and opportunities for improvement of the plan. After completing each test, needed updates to the plan should be identified and assigned. Updates are to be completed before the next test and are again tested specifically in the next round. In taking this approach TMCs have found the ability to maintain a highly accurate and valuable plan.

Documentation

Recovery and mitigation documentation has the dual requirements to be confidential and to be widely distributed. The information in the plan points out any vulnerabilities of the TMC system. By its very nature the documentation must have all the information needed to reconstruct the organization quickly. Network layouts, security infrastructure, systems complexities, internal procedures, and complete staff contact lists are some of the critical and confidential information that must be included in a plan. Any and all of this information may be used to infiltrate the TMC.

Wide distribution of the documentation is vital in order to educate the staff on the recovery and mitigation procedures that are in effect. The documentation is necessary for all of the testing, both scenario and full testing. Availability of the documentation is also necessary for ongoing updates as a result of error found in testing and changes needed due to development projects that are underway.

During system outages and emergency TMC relocation, the documentation must be available away from the operations center. Some TMCs make the documentation available through use of the Internet. In those cases, the documentation must be stored in servers that are not co-located with the TMC. Others provide the document in full or in part in hardcopy or on various softcopy devices such as CD or thumb drives.

TMCs that have addressed the issue of documentation security divide the document into sections as to the level of confidentiality for each section. All those receiving the documentation may not require all confidential sections, so each person is only issued the confidential sections that they require.

The documentation must be configuration managed in order to ensure that accurate copies exist. Each copy is numbered and assigned to a specific person. If the copy is delivered in hardcopy, each update is delivered with instructions of which pages to insert and which to delete. The version of instructions issued is numbered in order so that the documentation holder can identify if they have missed an update. Once updated the instructions are filed with the documentation. Au-

ditions of printed documentation are audited periodically to ensure that all documentation is up-to-date. Softcopy documentation may be reissued in whole with old copies retrieved and destroyed.

Alternate Site

Various TMCs have used a mixture of techniques at times when the TMC was not available. There are options to the classical hot site/cold site approach to recovery and mitigation which only further stresses the need to understand the requirements and goals of the TMC.

A solution that has been effectively used in several situations is regional assistance between agencies. An example of this cooperation was shown during the New York City Blackout of August 2003. The I-95 Corridor Coalition contacted member agencies that were not affected by the blackout to post messages informing motorists of the problem. The notification allowed the motorists the ability to avoid the effected areas, helping to relieve traffic congestion in the New York City area.⁹

Another approach used by several TMCs is that of working from alternative sites. These sites may include connecting into the system from the staff member's home or an alternate office arrangement. By connecting into the system from an alternative location, fundamental goals of the TMC may be handled without full access to the operations center. Depending upon the reason for inaccessibility of the TMC, this may prove to be a good solution. A large part of the decision to rely on this approach will be based on the requirements that are being solved with this solution and the location of the infrastructure including the servers. If the infrastructure is co-located with the TMC, connecting remotely to the network will serve no purpose in that the infrastructure in that case will still be unavailable.

SYNTHESIS OF RESULTS & BEST PRACTICES

As described earlier, there is a large range of recovery and mitigation efforts in place within the nation's TMCs. Communities have experienced emergency events that have resulted in systems outages in TMCs. In reviewing the events, TMC management have determined what practices have worked and those that have not worked; what to expect during emergencies and system outages; and how to prepare for future systems outages. Many of the successful practices have been instituted by individual TMCs. As with any other TMC system or installation, these practices must be reviewed in the context of the goals in the particular TMC organizations and the needs of the community for individual success.

Responding to Actual Emergencies

Several TMCs that have experienced major systems outages have developed specific procedures for the actions to take immediately. In most cases the system outage is unexpected, and the staff typically focuses on determining the scope and breadth of the case of the system outage. Most of the information that was being used for decision making was received from the media.¹⁰

Expect the unexpected. Issues on the streets are often different than expected. An example of this occurred during the Great Lakes blackout that occurred on a Thursday evening. Electricity went out, and all of the traffic signals went dark. The expectation was that the normal 4 pm traffic would be on the street. The traffic mitigation support needed would be in relation to the level of traffic normally expected with their 4 pm rush hour. What actually happened was that within 10 minutes of the blackout, all of the buildings emptied and the traffic that was expected to navigate

the streets during the typical evening rush hour period were on the streets at one time. In order to reduce the resulting gridlock, citizens took it upon themselves to go into the intersections and direct traffic.¹¹

An unexpected outcome of the New York City blackout was the effect of pedestrians on the traffic flow. The number of pedestrians that came into the streets at one time due to the power outage proved to further impede the flow of traffic. The sidewalks and walking areas could not accommodate the flow of pedestrians as they flowed into the streets and on bridges. The pedestrian flow exacerbated an already bad traffic situation.

An emergency plan that was already in effect in New York City directed individual police officers to specific intersections in order to manage the flow of traffic. An unexpected effect of the power outage was that many elevators within the city stopped trapping people between floors in the buildings. Rather than proceeding to their assigned intersections, police were called on to assist these people stuck in elevators. The police were not able to report to their assigned intersections to direct traffic.

A lesson learned from the New York City blackout was to define specific streets and bridges to be used for pedestrian traffic only, and other streets and bridges to be used only for vehicles.¹²

Many effects of the loss of power had not been expected by several TMCs. In reviewing what occurred and the resulting lessons learned from both the New York City and Great Lakes blackouts, it was determined there were a number of electrical connections that should have been considered for backup power that hadn't been. These included:

- u Phone system
- u Fueling system for public and private vehicles
- u Sump pumps for tunnels or roadway sections that are prone to flooding
- u Air conditioning for equipment room
- u Server hosting Email system
- u Radio communications system
- u Building security/electronic door systems

Power returning to the grid also resulted in unexpected events. Power returning to the grid was found to go on and off several times before it stays on. This puts extra stress on electronic equipment. Power may be restored in phases where some equipment is powered on with others still being off. The order of restoring power can cause some procedural issues.

Different equipment reacts differently when power is removed then restored. Some equipment must be manually reset. For equipment that needs to be manually reset, it is likely that this may have to be done multiple times as the power might cycle multiple times. Other equipment resides in whatever state it was before losing power such as a Variable Message Sign that holds the messages that were programmed. These messages which were appropriate for the point when power was lost may provide inaccurate information to drivers when the power is restored. TMCs must document and create procedures for these eventualities.

Communicating Information about the Outage

Both internal and external communications is critical during times of systems outage. The basic issue is that during these periods of time the normal communications structure within the TMC and the community is often not available. Communications with the recovery team is critical. Communications with other transit agencies such as paratransit has also been found to be important to the community. Additionally, communications with other agencies and first responders are frequently important, as is communications with the media.

A plan for this type of communications is critical, and this type of communications has been found to be of a low priority to the media during an emergency period. Other alternate procedures should be utilized which may include a predetermined mobilization plan for the staff. If the media is to be used for this type of communications, the budget should include an allocation for a media buy to communicate the message.

Getting the information out is of primary concern. A secondary concern is to make sure that the information communicated to the public is complete and accurate. In previous emergencies, a key way of assuring the accurate communications and complete information is to jointly communicate using an emergency operations center. Information from a centrally operated emergency operations center is more likely to be picked up by the media. But, having a budget for media buying for an emergency operations center is also a useful expenditure.

Before an emergency situation occurs, the TMC should build external relationships with other appropriate agencies and media contacts. Agencies should include law enforcement, state and local emergency management centers and other non-transportation agencies as well as other TMCs. A system outage is not an appropriate time to initially meet with these external resources. By meeting with these people in advance, an understanding and documenting of the possible procedures and usage of these entities is able to be accomplished.

Areas Normally Overlooked

While working through emergencies, there have been a number of issues that TMCs have found that are normally overlooked which should be addressed in a plan. One of these that came to light during Hurricane Katrina was support for the family of the needed staff member. Various methods can be deployed including moving families, staff members and providing care for the children during period like this.

For periods of loss of full functionality of the TMC or community-wide emergencies, stocking emergency supplies is critical. Food, water, flashlights, batteries and radios have been found to be important to sustain the staff members and allow the systems to be maintained and recovered as efficiently as possible.

Many TMCs and other organizations that have experienced severe system outages feel that an important function that is frequently overlooked is the continued evaluation of the backup generation capacity. As the infrastructure of the operations center and the equipment that is critical changes the amount of emergency power needs will change correspondingly. There are also changes to the specific locations to which the emergency power is to be delivered.

Lack of power was found to cause issues for river traffic as well. The Great Lake blackout found that the lack of electricity resulted in draw bridges not being able to be raised -- again, an issue that was not contemplated or for which no planning was accomplished.¹³

Low tech solutions that have been used in the past should be considered as backups to the current higher technology that is currently being used. Examples of low tech solutions may include telephones that are connected directly to the central office and do not require electricity, dial-up modems and manual procedures.

Support for the staff members that have been found to be important during periods of relocation include items that provide comfort to the staff member and their families. These include items such as lists of restaurants, gyms and religious organizations local to the living arrangements.

Businesses Unable to Operate

In planning recovery and mitigation strategies for TMCs and mobility, thought must be given to businesses and organizations in the private sector that will change their operations or not be able to operate at all. As pointed out earlier, the flow of pedestrians and traffic are likely to change during emergency situations. Workers will leave their places of business both because of the lack of utilities available to their workplaces and/or because of concern for their families and property.

As found in many community-wide incidents gas stations are frequently closed. With a large egress of vehicles, all available gas will be purchased quickly and stations will close. In some cases, the lack of electricity pumps will no longer operate which will also close the gas stations. Effects of this will be long lines at any stations that are open, the need for police support at these stations, sufficient gas not available for emergency responder vehicles and motorists running out of gas with their vehicles blocking the roadways.

To make the situation worse, during the Great Lake blackout, half of the Cleveland-area American Automobile Association was not able to operate due to the in-truck computer network being inoperable because of the blackout.¹⁴

There have also been some recent examples where private organizations have also assisted in emergency situations where utility infrastructure was not available. During the aftermath of Hurricane Katrina, communications infrastructures were not available. Both Walmart and Coca Cola had proprietary infrastructures established. Walmart made their communications infrastructure available for use by emergency responders. Coca Cola made their network available to people in the area to use for personal messages.

Results of Survey Questions and Interviews

As a part of research for this technical report, surveys were sent out to TMCs and a number of management staff of TMCs was interviewed on recovery and mitigation within their organizations. One 911 center was also interviewed on the same subject to understand the extent of recovery and mitigation that government operations centers can accomplish. In order to receive accurate information, all organizations were guaranteed anonymity in their responses.

The range of processes employed, knowledge of recovery and mitigation and commitment to planning range from none to operations centers that measures up to any other operations center in the country.

By and large, a systemic approach was not found towards linking specific goals of the TMC with recovery or mitigation plans. Recovery and mitigation planning fall into three categories:

- u No plan due to it not being a priority, no budget or lack of knowledge of the issue

- u Plan in place based on what each person in charge had decided to add to it over the years
- u Plan in place that was accomplished by a formal program of plan development

Various mitigations have been identified as being in place within communications, hardware, and infrastructure. In the communications area, several TMCs have reported to have multiple communications paths that provide redundancy. Some of the redundancy is manual and some of the redundancy is automatic. With manual redundancy, separate lines can be configured for used or separate equipment may be used if needed. Automated redundancy includes technologies that provide for a secondary path for all communications that is always available. In this case, communications will either follow the best route or switch to the alternate path as needed.

Hardware mitigations consist of backup hardware being available. They may either be always online, or the hardware may be always ready when needed to be activated. Some TMCs have expressed that the backup hardware is the previously used, smaller version of the same hardware that is currently being used. When the plan includes this type of backup, extensive testing should be performed to ensure that the smaller, older model of the hardware is compatible with the current hardware and infrastructure. There are normally upgrades to functionality that the system may be using that does not exist in the older system and may make the older version of the hardware unusable as a backup system.

Infrastructure mitigations include UPSs for power, physical security, and reinforced buildings. Also addressed are infrastructure improvements such as sprinkler systems for fire protection. It should be remembered that if the mitigation for fire is a sprinkler system, the mitigation itself is likely to cause a significant systems outage if activated.

With a propensity towards cyber crime, an important mitigating factor in all operations centers is data security. With data security, most TMCs report the use of firewalls and virus protection. Related policies such as who has access, when access is turned off for an individual, logging, internet access, e-mail usage, and password security are often not as tight as are necessary.

Universally, planning was recommended by TMC management. This includes both those that had recovery and mitigation plans and those that did not. With that, there was a difference in opinion of the amount and specific type of planning that is necessary. Some TMCs felt that their plan was a portion of a larger emergency planning function of the municipality while others consider that the plan fell under their specific purview.

It was uncommon among TMCs to have their plans reflect directly on a stated, codified mission of the organization that has been approved by management. More likely, the plan reflects the level of knowledge of the subject by middle and senior management. Often this means that a technique supported by the industry is instituted without full knowledge of how to integrate it into the operations. This often results in an expenditure that has been made in a technology without the expected payback in benefits.

Preparation of the recovery and mitigation plans varied widely between those that were developed and updated by consultants, to those developed and updated by a central specialized area, to those that had internal staff develop and update the plans. Each of these variations was for different reasons. Consultants were found to be used to produce the plans in conjunction with other work being done such as building a new TMC. They have also been brought in to do this work when the TMC staff was overloaded with existing work.

Some municipalities have prioritized recovery and mitigation planning high on their project list and require all departments to be part of one consistent plan. In these cases, a specialist has been employed by the municipality. The specialist then runs the project and uses the staff members as the subject matter expert.

In most cases, current TMC staff was asked to write a plan as another task that needs to be completed. These staff members have little to no training in the theories of recovery and mitigation, and were not required to follow any specific format or structure. The plans turn out to be fundamentally one which will document the process that is used by the TMC. Management, in some TMCs, have also expressed that they feel that internal staff must do this planning to keep them educated, knowledgeable and empathetic towards the issues.

Ongoing maintenance of the plan shows significant differences in commitment and execution by the TMC. On one end of the spectrum are the TMCs that have ongoing maintenance built into all procedures with weekly meetings to discuss and establish action items for improvement. This requires an ongoing budget commitment to the program. On the other end of the spectrum are TMCs that feel that their plan is in relatively good shape and time permitting, will get back to reviewing and updating the plan.

Some levels of backups are reported to be accomplished by most all TMCs. The question remains -- are the appropriate types and frequency of backups are completed and if the backups are tested? Backups must be tested by doing a restore and attempting to run the systems using the backups. Without testing in this fashion, there is no assurance that the backups are being completed correctly and that the correct files are being stored. There is a great difference found in the location of storage of the backups. Some TMCs store the backups on-site, others store it in another part of the same building and still others have them stored at a manager's home. A few have them stored in sites that are appropriately conditioned for storage of computer media and may be accessed if needed for a recovery.

Appropriate ongoing testing, like maintenance, requires a budget commitment by the TMC. Some TMCs feel that they do not need to test because the backup site is always running and is periodically used. Others have expressed that there are enough recoveries that are performed due to actual outages at their operations center that there is no need for scheduled testing. Yet others have the plan on the shelf and will take it off when needed for a recovery effort, if ever needed. Finally, some small numbers of TMCs perform periodic, scheduled testing of both scenario desk testing and full onsite testing. Testing in this fashion is an expensive undertaking, but this is the only method to be assured that the plans are adequate to support the TMC in case of a significant system outage.

When performing full tests, it is appropriate to use the established alternate sites for this testing. Several TMCs expressed that their expectations are to have the staff working off-site and dialing into the current computer infrastructure. If the location where the computer infrastructure resides has a loss of utilities (i.e. power, communications lines), the alternate site becomes invalid for this purpose.

Included as a portion of several TMC recovery plan is the use of a federal government program for prioritization of telephone calls. By preparing for communications during community-wide disasters the TMC is able to have their staff equipped for both landline and mobile communications that will be given priority over other calls being made. The Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) programs have been es-

tablished to allow critical personnel this ability. TMCs that have not signed up for this program have done so primarily because of lack of knowledge of the program. The cost of participating in these programs are low, the primary issue is to show the appropriateness of inclusion.

Actual Experiences

A number of community-wide emergencies have occurred over recent years that have required TMCs to exercise recovery and mitigation plans. Mother Nature, infrastructure faults and terrorists have combined to require TMCs and other operation centers to work with downgraded facilities or at alternate sites.

During periods that include loss of communication and power, there is also a loss of use of the roadway equipment. TMCs no longer have access to pictures of traffic flow using CCTV cameras, data on traffic movement from sensors or the ability to communicate with the public using DMSs. Traffic signals, lane use signals, ramp meters and other automated traffic control devices have gone dark and are of no use in helping traffic movement.

Following a community-wide disaster of this type, complete and accurate information is imperative. Information is required by the agency officials in order for them make decisions based on facts. The public is also interested in being kept informed both in order to make informed decisions on their personal movement and their property.

During Hurricane Katrina, the lack of communications was the most significant issue that had to be overcome. Communications redundancy, both voice and data, was problematic due to a lack of planning. Communications during an emergency situation of this type is required with internal staff, other governmental organizations within the community, and the public. Lack of infrastructure began the communications problem through the loss of central offices, telephone wires and power. The issue was made worse because there is no agreement on data communications protocols or established interdepartmental communications frequencies.

Even when communications issues have been considered, unexpected issues have been encountered.

- u The Louisiana State Police reported that during the aftermath of Hurricane Katrina, cloud cover restricted satellite communications. Satellite phones, which require specialized knowledge of use, were not able to be used to the plan expected levels.¹⁵
- u During Hurricane Katrina, emergency personnel found that there were 10 different frequencies that were being used by different agencies. The various pieces of radio equipment is incompatible with each other. Much of the communications equipment is 30 years old or more.¹⁶ This led to limited command and control that could be exercised.
- u During the New York City blackout, 800 telephone numbers were established by both TRANSCOM and New Jersey Transit for use by the staff of various agencies to receive current information and to conduct conference calls.¹⁷
- u In order to keep the public informed during the events of 9/11, the Virginia Department of Transportation (VDOT) used a centralized Transportation Emergency Operations Center (TEOC) to distribute information. The information was distributed to VDOT offices, other Virginia government offices, the media and the public using various methods including continuous postings on a VDOT web page.¹⁸

Best Practices

A number of TMCs have experienced significant systems stoppages. Some have been as a result of a community-wide disaster, some as a localized event. As a result of either case, a significant number of “best practices” or “lessons learned” have been generated. This list is an attempt to “allow others to close the barn door before the horse escapes”. Each individual item should be considered in context of the mission of the particular organization and the TMC as well as the environment in which both exist.

Management

1. *Management commitment* is universally considered an important best practice. Senior management of the TMC and the agency as a whole should adopt an attitude that the operation is vital to the well-being of the community and must be available no matter what happens. *This attitude must be communicated to all staff members* at every level of the organization.
2. The commitment must extend into *funding for the initial planning project and continued funding for ongoing testing and updates*. A commitment by management of the importance of recovery and mitigation without the associated funding has little effect on the process and will mean little to the staff.
3. Senior management should also encourage and fund the creation of critical systems that provide for identification of systemic problems as well as ease the correction of these problems. This will help in the rapid recovery in cases where systems problems occur.
4. The codification of several policies by management is also vital to the ongoing success of the program and its outcome. Best practices in policies that have been identified by TMCs have included several that allow action during an emergency situation rather than staff members considering different options. They include:
 - a. *Establish internal coordination of the operations* during emergency situations
 - b. *Develop a consistent policy for toll and fare collection* with the possibility of tolls and/or fares to be eliminated during these situations.
 - c. *Establish and disseminate a policy for displaying messages on variable message signs* including wording of messages to be posted and the associated locations.

Planning

5. The planning process must begin with the *development of a mission statement*. Much the same way that the system engineering begins with requirements in order to understand what a system is being proposed to accomplish, the planning process for recovery and mitigation must begin with a mission statement that defines the goals and objectives of the TMC. *The mission statement must be approved by senior management* as another facet of their buy-in to the importance of this process.
6. As a part of codifying the mission statement, a quantification of allowable downtime should be determined. This is a first step in documenting a procedure to be followed in order to determine if a recovery situation should be declared. *The line of demarcation be-*

tween a temporary outage and system outages that require a declaration of this type is critical.

7. Along with the mission statement, knowledge of the multi-model transportation system must be kept in mind. *Specific usages of the roadway system are vital in the planning which includes routes for first responders, evacuation, and the like. An understanding of and coordination with the transit system provides options in development of the plan. Possible movement of pedestrians during an emergency situation must also be factored into the plan to provide for their safety as well as allow for the most optimum mobility for all people.*
8. An unending assortment of causes may have the effect of a system outage. These include, but are not necessarily limited to:
 - a. Fire
 - b. Power outage
 - c. Epidemic that disables significant amount of the staff
 - d. Critical weather situation
 - e. Building being condemned
 - f. Riots in the community
9. There is no method of anticipating all of the different combination of events that may create a system outage. Therefore it is imperative that *the plan be written generically so that any cause of system outage is supported.* Rather than addressing any possible cause, the plan is addressing the related effects of the outage.
10. *Planning should not neglect low-tech solutions within the development. Older technologies may be able to backup current high-tech solutions. The use of POTS (plain old telephones) connected on an analog line directly to the telephone central office is an example of older technology that may be used as a backup. Items that include these low-tech solutions should be periodically inventoried to ensure that adequate amounts are being stocked. This should include such basics as flashlights, batteries, radios, food and water.*
11. *A worse case scenario should be planned for in order to cover all possibilities. Losing the complete TMC along with access to any documentation and files located in the building, all communications lines, power, computer servers, and critical staff along with the use of all roadway instrumentation may be a worse case scenario that may be the basis for planning the TMC recovery. The plan should also assume that all communications lines have been lost and will not be available for the immediate future.*
12. During the planning process it is important to remember that *no matter the level of mitigation that has been designed into the operations, the device or architecture could fail.* This has included a power strategy that, during the Great Lakes blackout failed even though there was quadruple redundancy in place.
13. From this point the planning process may begin, being designed in accordance with that mission statement. A function provided by the plan is *the relative prioritization of restoration activities.* Once the mission is fully understood, documented and signed off the information may then be used to identify the relative prioritization of these activities.

14. During the planning process *consideration should be given to ITS functionality that could aid the communities*. Priority may be given to restoration of the particular devices needed to support this functionality and/or additional resources should be dedicated to its mitigation.
15. *The use of ITS equipment for keeping the public informed should be considered. Portable ITS equipment may be found to be valuable during community-wide emergencies*. If this type of equipment is planned for use consideration should be given to *physically protecting the equipment* such as chaining it down if high winds are expected.
16. With the advent and proliferation of home computers and the Internet, the *concept of redundancy should be rethought*. Some TMCs are considering a virtual operations center as an alternate site when needed. The staff members may work from their home or from a hotel in the case they are evacuated.
17. *Individual relationships between people become more important during emergency situations*. The relationships are not always only within one department or division; they may extend into different agencies that work together during these situations. Planning for and assisting in creating these relationships are helpful to the recovery effort.

The Mitigation Plan

18. *The plan should be detail-oriented with procedures that are easily and efficiently implemented* resulting in the staff being able to quickly understand and carry out the instructions set forth. *Preparation in advance for an emergency makes the day-of-event decisions easier to resolve and manage*. The plan should include assignments that *specify the person authorized to declare a disaster and to contact each service to authorize it being started, restarted, and/or redirected*.
19. Provisions should be made to *empower specific positions within the staff to make and communicate decision during the recovery situation*. No matter the completeness of the recovery plan there will always be changes that are needed upon true execution.
20. The TMC plan should *account for a multi-agency response to a community-wide emergency*. *Inter-municipality responses to community-wide emergencies* should also be considered. This may include responses that are across state borders. *Additional technological solutions should be reviewed that will enhance this type of coordination*. Included may be devices such as radio repeaters that change frequencies so that different agencies may continue to use existing equipment with the ability to communicate with each other.
21. *Methods, processes and procedures for returning to the TMC should also be included in the plan*. Many of the same decisions, complexities and actions taken in moving the operations to an alternate site are needed in order to return to normal operations. By documenting this in advance the management may concentrate on the day-to-day operations rather than planning on the fly when and how to return to the existing or new operations center.
22. In addition to the hardware and software, *consideration in the plan should be given to the people that will be affected*. In the case of the alternate site being in a different city than the primary TMC, staff members may be asked to leave their home and family in order to perform their jobs. When the system outage is due to a community-wide emergency it

may require the staff member to leave their family and property that are in danger. Some organizations have reported making provisions for families to join the staff member at the off-site locations.

23. Additional *reviews should be held after activation of the plan* in either a test or actual outage mode. In either case, a punch list of errors and improvements should be generated for required updates in the plan. The items should be prioritized and assigned to the appropriate people with periodic status reports to a central manager.
24. If an emergency situation is expected due to such things as hurricanes or planned power outages, *cross-agency meetings should be held as early as 72 hours* before and continue periodically until the outage occurs. The meetings should include as many agencies as practical including all effected areas, which in many cases will transverse boarders. These meetings may be used to put inter-agency cooperation measures into place.
25. When emergency situations occur without warning, the *procedures within the plan should begin with what may be accomplished immediately*. If power is lost, *procedures that may be accomplished without the use of power should be executed*. An example of procedures that may be accomplished without power and is critical to accomplish as quickly as possible is *an immediate setting of priorities*.

Power

26. *Periodic tests of the backup power* are essential to the mitigation of risk. Some TMCs perform the test weekly, having the TMC run on backup power only, during the heaviest usage period. In this way the TMC can be assured that the backup UPS and generators are working properly and supplying the complete installation with power.
27. In deciding the correct circuits for which to provide backup power, the best course of action is to *provide backup power for the complete TMC*. In providing the backup power to the complete installation, there is assurance that power is available for all equipment that needs it. This also provides the ability to periodically turn off utility power and which will provide an absolute test of the backup power system. The alternative is to do an analysis of specific circuits that require backup power and enable only those circuits. Analysis and testing of this type of installation contains significant complexity.
28. No matter which method for deciding on the amount of backup power that is needed is used, *the amount of backup power being provided should periodically be reevaluated*. The environment within the TMC changes constantly. Equipment is added, equipment is replaced and power consumption changes. A period should be set to reevaluate the power needs and upgrade the power backup solution as is found to be appropriate.
29. During an emergency situation, *backup power must be provided to both the TMC and ITS equipment in the field*. Availability to the systems in the TMC are of little value to the community if field equipment is unavailable due to lack of power. Of primary concern to some TMCs is the use of CCTV cameras to monitor the conditions. This equipment requires power and communications infrastructure to operate.
30. *Traffic controllers and signal heads should be reviewed as to the need for backup power*. During emergency situations the signal heads at intersections are either dark with no traffic control, or intersections are staffed by police officers who manually control the traffic

flow. In several recent emergency situations where there was no power for the traffic control equipment, police officers were being used to free people stuck in buildings and were not able to be used for traffic direction. In one case drivers left their vehicles and directed traffic themselves.

31. *Portable signs that may be used at strategic locations* in order inform drivers of evacuation routing, conditions in particular areas and the like may be run with backup power. This has been found to be a good means of communications to the public. Positioning the signs at strategic points adds to the ability of the TMC and emergency management officials to disseminate a message accurately to all those affected.

Communications

32. TMC communications systems pose their own unique mitigation issues. A primary mitigation method is the *use of multiple methods of communications technologies from multiple providers*. With the constant changes that are taking place in communications technologies there are many different types of technology that may be used such as SONET, T-1, DSL, satellite backhaul and dial-up connectivity. By having multiple types of technology available for communications to the TMC, there is a much higher likelihood that one of the technologies will be available.
33. *Availability of older forms of communications* such as POTS (plain old telephone system) connected directly to the telephone central office and portable radios allow for a different type and often a more resilient backup for communications.
34. *Equipping key personnel with personal communications equipment* may allow important communications to continue, even with area-wide communications problems occurring. Possible communications equipment includes laptops, cell phones and Blackberries. By having this type of equipment available, critical communications may be able to be maintained during an emergency situation.
35. In evaluating significant disaster situations, the number one issue cited is often communications. The communications issues include lack of communications and misleading communications.
36. *Additional communications options should be explored for use during recovery situations*. These may include services such as priority telephone services (WPS), priority cellular services (GETS), push-to-talk services, satellite telephone, and personal email/text messaging. Utilization of services of this type allows for alternate means of communications during emergency situations.
37. *Review potential possibilities of and placement for advanced technology to help communicate with the public*. Possible technologies may be email, text messaging, web sites, or private signage. The ability to communicate appropriately to the community is helpful in keeping the community calm and allowing the citizenry to act in a manner that is desired by the emergency officials.
38. *Interpersonal, inter-organizational and interagency communications should be established and strengthened before an emergency event occurs*. Having productive communications with media outlets, other governmental agencies, peer transportation agencies in the region and corporations that have a significant presence in the community helps get

the message out to appropriate people. Organizing responses by all of the organization to the emergency will help maintain the community calm and can be used to orchestrate a consolidated approach to responding to the emergency. Coordinated decisions such as when and how to release employees or requirement of taking time off will assist in mobility issues that occur.

39. A *community-wide HAR system* will provide a consistent message for community consumption. With appropriate advertising of this type of service, the community will be using their radios tuned to this particular frequency to receive local important information. The directions that the emergency team wants to communicate will then be made available consistently to the public.

Other Mitigations

40. In order to help mitigate the possibilities of having a disaster, a number of best practices have been sited. As with any risk mitigation, these procedures will assist in lowering the probability of having an emergency situation, but it can not eliminate the possibility of a system outage.
41. A primary mitigation of system stoppages is to *construct the TMC as a “bunker”, locating it outside of any floodplains* or known area with problems. It should also be *located in areas that may be supplied with service by multiple power substations and multiple telephone central offices*. The TMC should be equipped with appropriate physical security devices in order to permit access to only approved people.
42. *Backup power to sustain the complete TMC is a valuable mitigation* for the periodic power failures occurring in all areas. Both an uninterrupted power supply (UPS) for immediate backup, and a generator for longer-term backup are needed. UPS are sets of batteries that are capable of maintaining power without any interruption for a short period of time. The period of time is long enough for power generators to start and take over supplying power.
43. The use of TMC’s *personnel home computer infrastructure should also be used as an approach to recovery*. “Cisco Systems found that using DSL lines and VPNs to employees' homes has helped the company maintain service during ice storms on the East Coast and the SARS epidemic in Asia.”¹⁹ This approach will function as both mitigation and a recovery strategy for the TMC.
44. When using portable ITS equipment such as signs and generators that are located outside, this *equipment needs to be secured in place*. High winds and flooding can cause additional damage to this equipment when it is thrown around.
45. During emergency situations all emergency response agencies require some number of vehicles on the streets. *When power to a community is lost, fueling facilities can no longer dispense gasoline* because the pumps are powered by electric power. Fueling facilities that are used for emergency response vehicles should be a candidate for backup power.

Training

46. *Training and practice exercises should be held* to familiarize the staff with the recovery plan. The objective is to train personnel in the tasks that they are to perform and the reasons behind them. With this training, staff members can more easily make decisions during actual recovery situations using complete knowledge of the topic. *The practice should include an inter-agency rehearsal of the emergency response plan* which will also add to the complete team's camaraderie.
47. The training should be held to *cross train staff for additional job functions* if required. In order to make the TMC self-sustaining, *training should include all systems and equipment*. Training to these levels allows the TMC to depend solely upon internal staff, not having to rely on any specific people or specific contractors.
48. *Desktop testing should be held periodically* to allow personnel to logically think through different possible scenarios that may occur to cause an emergency situation. This type of testing should be an inter-agency activity in order to involve all those to respond to community-wide events. Cross-boarder agencies should be included in order to think through regional approaches to emergencies.

Documentation

49. *Care should be given to the production and storage for the plan that is produced*. The plan is of little use if it cannot be accessed or read when needed. The plan must be accessible to appropriate staff members. Confidential information within the plan should be available to only specific staff members. If the plan is going to be available softcopy, one or several hardcopy version may be required to begin the work of recovery before computers and networks are available.
50. As part of a TMC plan or through reference other related plans should be available. These include *clear procedures for evacuation of personnel* from the TMC if necessary and an *emergency response plan*. Each of these plans may be under the purview of other organizations, but verifying their existence and including them by reference is recommended.
51. An important part of a TMC's effort in keeping their plan up-to-date is an ongoing maintenance process. A beginning to this process is to *make updating the recovery and mitigation plan a part of the normal change process within the organization*. In this way, when any changes are made to the TMC or the outside environment of the TMC, analogous changes are made within the plan.
52. Management of and action items for *updating the plan should be a function of a periodic status meeting*. In these meetings, mid-level managers set a direction for the recovery and mitigation plan. Tasks are assigned and monitored on a periodic basis, which have been set by some TMCs at weekly or biweekly.

Working Relationships

53. Some final best practices speak to external relationships that must be established and maintained prior to an emergency situation occurring. These include those within your municipal government, those in governments within your region, those in the private sector and those with the public.

54. *Involvement with the local law enforcement agencies, emergency management agencies, transportation agencies and other non-traditional agencies are important* in order to give the citizens a consolidated support structure during emergency situations. Communications with local agencies should include your state and local agencies.
55. In order to achieve a good working relationship for emergency situations, *the communications must start during normal times*. A working relationship of this type will allow for sharing resources and equipment on an inter-agency basis.
56. *Good working relationships with other regional transportation agencies have been shown to be valuable*. During critical situations, transportation agencies around your region can warn drivers of the situation and recommend avoiding the effected area.
57. It should be remembered that, although cooperation among regional agencies is a good idea, *depending upon these agencies for redundancy must be approached with caution*. These agencies install infrastructure to support their own needs. It is unusual that an agency will be given the funding in order to keep additional equipment in working order for another agency to occupy in case of emergency.
58. *Establishing a good working relationship with private companies* that have a significant presence in your municipality is a good idea. The relationship may be used to coordinate communications and public action during emergency situations.
59. *Open lines of communications with the print, television, radio and internet media is important during emergency times* in order to have support for the information that is to be disseminated. A positive working relationship during normal times can only be a help in moving forward with the mission of the organization.

Best practices, as other information presented must be measured against the mission, goals and infrastructure in place for each individual TMC. The best practices that have been discussed here are those that have been determined primarily by TMCs that have experienced emergency situations. These best practices should be considered, but not arbitrarily.

⁴ Dan Verton, *Black Ice: The Invisible Threat of Cyber-Terrorism*

⁵ Warrick, Cathy, et al, *IBM TotalStorage Business Continuity Solution Overview, International Business Machines Corporation, 2005*

⁶ Swanson, Marianne, et al, *June 2002*

⁷ DeBlasio, Allan, et al, *Effects of Catastrophic Events on Transportation System Management and Operations: August 2003 Northeast Blackout, Great Lakes Region (Final Report), DOT-VNTSC-FHWA-04-04#, May 2004.*

⁸ DeBlasio, Allan, et al, *Effects of Catastrophic Events on Transportation System Management and Operations: August 2003 Northeast Blackout, Great Lakes Region (Final Report), DOT-VNTSC-FHWA-04-04#, May 2004.*

⁹ DeBlasio, Allan, et al, *Effects of Catastrophic Events on Transportation System Management and Operations: August 2003 Northeast Blackout, New York City (Final Report), DOT-VNTSC-FHWA-04-04#, March 2004.*

¹⁰ DeBlasio, Allan, et al, *Effects of Catastrophic Events on Transportation System Management and Operations: August 2003 Northeast Blackout, New York City (Final Report), DOT-VNTSC-FHWA-04-04#, March 2004.*

¹¹ DeBlasio, Allan, et al, *Effects of Catastrophic Events on Transportation System Management and Operations: August 2003 Northeast Blackout, Great Lakes Region (Final Report), DOT-VNTSC-FHWA-04-04#, May 2004.*

¹² DeBlasio, Allan, et al, *Effects of Catastrophic Events on Transportation System Management and Operations: August 2003 Northeast Blackout, New York City (Final Report), DOT-VNTSC-FHWA-04-04#, March 2004.*

¹³ DeBlasio, Allan, et al, *Effects of Catastrophic Events on Transportation System Management and Operations: August 2003 Northeast Blackout, Great Lakes Region (Final Report), DOT-VNTSC-FHWA-04-04#, May 2004.*

¹⁴ DeBlasio, Allan, et al, *Effects of Catastrophic Events on Transportation System Management and Operations: August 2003 Northeast Blackout, Great Lakes Region (Final Report), DOT-VNTSC-FHWA-04-04#, May 2004.*

¹⁵ United States. Cong. House. *A Failure of Initiative: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina*. 109th Cong., 2nd sess. 15 Feb. 2006.

¹⁶ United States. Cong. House. *A Failure of Initiative: Final Report of the Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina*. 109th Cong., 2nd sess. 15 Feb. 2006.

¹⁷ DeBlasio, Allan, et al, *Effects of Catastrophic Events on Transportation System Management and Operations: August 2003 Northeast Blackout, New York City (Final Report)*, DOT-VNTSC-FHWA-04-04#, March 2004.

¹⁸ Pearce, Vince, "Securing the Roads",

¹⁹ Crosman, Penny Lunt, "A Watertight Plan", September 1, 2005,

<http://www.itarchitect.com/shared/printableArticle.jhtml?articleID=169400810>

3

THE PLANNING PROCESS

Chapter 3 Purpose:

To review the reasons for and process of executing the project of planning for recovery and mitigation of systems outages. An understanding of the personnel involved, documentation, funding, and objectives of the recovery and mitigation are covered in order for the executive sponsor to understand the various issues involved in this process. This chapter also addresses the necessity and ongoing commitment required for continued support of the plan.

Chapter 3 Key Message:

- u Mitigation and recovery of TMCs begins with planning
- u An appropriate plan that is tested and updated is key for the TMC management in times of system outage
- u Preparation and maintaining an appropriate plan requires time and effort

OVERVIEW OF THE PLANNING PROCESS

The planning process for recovery and mitigation is felt by many within the TMCs, other agencies and businesses as the complete project. Planning is a critical piece of the project, but should not be the complete project. In instances where the planning process is considered the complete project, the deliverable is often documentation of the current procedures with thought given to restoration using obvious scenarios.

Planning is a mid-point in the project. Before planning is attempted, a number of tasks must be accomplished including management commitment and funding, establishment of a mission and goal statement, and establishing a team.

The following process diagram provides a framework for the planning process. Each step in the process is discussed further below, with the exception of “Determine Mission and Priorities”, which was discussed in Chapter 2.

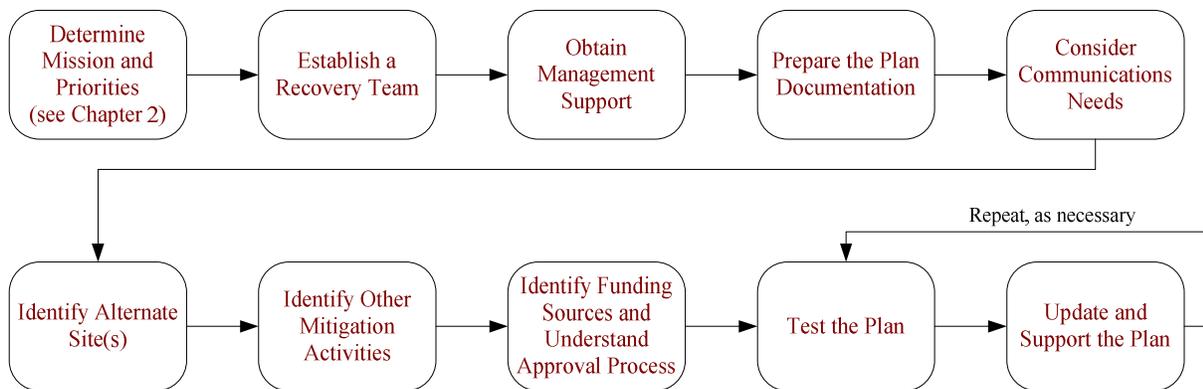


Figure 1 - Planning Process Diagram

PLANNING GENERICALLY FOR ALL TYPES OF OUTAGES

A plan should address recovery and mitigation without having to be specific to any particular cause of the outage. There is no way to realistically define all of the possible causes of systems outage. Any number of combinations of events may cause a system outage. The planning exercise should assume a worse case scenario. If a system outage occurs that is not as bad as this assumption, the team is able to relatively easily remove functions to be accomplished in order to match the actual occurrences.

As was noted in the Best Practices section of Chapter 2, an important worst case scenario that should be designed into the planning process is that the TMC loses all communications, both voice and data. Several TMCs have reported from actual experiences that the worst issues encountered in previous major systems outages was caused by a lack of communications. Planning should prepare for a loss of communications even if the current communications is mitigated through multiple feeds, technologies, and sources.

The ultimate goal of a recovery and mitigation program is to ensure continuity of operations (COOP). Specific operations that a COOP addresses will be different for each TMC and will be based on their mission and goals. No matter the goal of individual TMCs, their particular operations are important and must be maintained.

The federal government considers continuity of operations, within their operational divisions, to be critical for a number of reasons that include:²⁰

- u Ensuring continuous performance of essential function and operations during an emergency
- u Protecting essential facilities, equipment, records, and other assets
- u Reducing or mitigating disruptions to operations
- u Reducing loss of life, minimizing damage and loss of service to customers

The Executive Branch of the federal government has felt this to be an important enough issue that a Federal Preparedness Circular (FPC 65)²¹ was issued outlining the COOP service levels of all Executive Branch Operations. FPC 65 requires these organizations to maintain plans that will:

- u Maintain a high level of readiness
- u Be capable of implementation both with and without warning

- u Be operational no later than 12 hours after activation
- u Maintain sustained operations for up to 30 days

TMCs must plan to provide for an orderly recovery in case of a system outage in order to resume operations, and meet the mission and goals set out for the organization. An important place to begin planning is to understand the scope of the projected plan which can range from recovery of one or several applications to complete restoration of the TMC.

As stated by David Comb, the CIO of the USDA, in speaking about recovery from Hurricane Katrina,²² the success of the ultimate recovery is based on People, Plan, and Practice. The people involved in recovery must be committed to the objectives. They must also be knowledgeable on the topic of recovery and understand how their work fits into the complete recovery scenario.

Once the plan is completed, ongoing practice is critical. Practice serves several purposes. Testing of the plan is a critical and obvious outcome of practice. At the end of each testing cycle a list of plan improvements are generated which leads to upgrades and improvements. Other purposes include continued training and team camaraderie. Keeping team members fully trained in their recovery function and cross trained into other functions continue to reduce risk to the organization. The camaraderie between team members will help communications and cooperation in the event of a real systems outage.

The Executive Branch of the federal government indicates in FPC 65 that the minimum guidelines to be included in a COOP plan are:

- u Delineate essential functions and activities of the organization
- u Outline decision processes for determining appropriate actions in implementing the plan and procedures
- u Establish a list of capable personnel with proper authority for needed functions
- u Personnel know that they may need to relocate and are available at any hour or any day for this task
- u Personnel accountability during the emergency situation
- u Operational capabilities will be restored within 12 hours
- u Alternate operations can continue for up to 30 days, if needed

A plan that defines actions to this level will minimize disruptions of operations while assuring stability of the TMC and provide a recovery that will be efficiently executed. The resultant actions of executing a well designed plan will be to provide stability while minimizing effects of the system outage within the community and TMC. It will delineate personnel responsibilities and authority while reducing the need for decision-making during the restoration process. Personnel will understand, in advance, what will be expected of them during the outage. The end result will give the TMC the ability to meet agreed upon service levels.

The plan must address system outages within normal operations as well as during community-wide emergency situations. The mission and response activities are likely to be different during community-wide emergencies than during normal operations. The TMC has an infrastructure and access to instrumentation that can be made available to first responders to help them do their job more efficiently and effectively. An understanding of the flow of traffic along with pictures of

specific areas from CCTVs will allow for better management of the disaster. The plan for recovery and mitigation must take into account the specific mission of the TMC during these times of disaster. In combining resources of the TMC with those in emergency management will result in a positive effect on the community as a whole.

Team

Planning for recovery must include training and the possible mobilization of an appropriate team of people to execute recovery efforts. IBM has recommended in their Redbook series of manuals that the team includes sub-teams, each responsible within their own levels of expertise.²³ These sub-teams include:

- u Management team
- u Business recovery team
- u Departmental recovery team
- u Computer recovery team
- u Damage assessment team
- u Security team
- u Facilities support team
- u Administrative support team
- u Logistics support team
- u User support team
- u Computer backup team
- u Off-site storage team
- u Software team
- u Communications team
- u Applications team
- u Human relations team
- u Marketing/customer relations team

In addition to these specialties, there are a few other functions will be useful during a recovery situation. By having these specialists as part of the team, the process will be improved. The additional staffing include:

- u “as many as can be spared from IT. Make sure there is a management level person from IT on the team”²⁴
- u Building Support/Maintenance department representative
- u Finance/Accounting department management

There is not a specific reason to set the recovery team up in exactly the fashion mentioned. More, it is important to have each of these functions represented on the recovery team. Each of the teams has specific functions. Some need to be involved for the full period of system outage. Other teams’ primary function at the beginning of the outage, while other teams may be needed primarily if the system outage persists for a long period of time.

A Communications Leader should be selected. There should be only person that will communicate both internally and externally. In having this function handled by only one person, it enables a consistent message to be communicated. The person may be within the TMC or may be from a different department. Even if they are not part of the TMC organization, they are a member of the TMC’s recovery team.

Responsibilities of each of the teams must be specified. Codification of the responsibilities may be within departmental policy or may be within recovery procedures. In either case there are important decisions covering responsibilities and authorities that can and should be made in ad-

vance of a system outage. Some of these must be handled before the system outage; others are the responsibilities of authorities during a system outage. These include

- u Roles and responsibilities of each of the specific sub-teams. This allows personnel to make decisions at their level.
- u Training requirements for each team member
- u Exercise and testing schedules, both for the TMC and interagency
- u Plan maintenance schedule
- u Frequency of backups and storage of backup media

Backups for each of the individual team members may be determined. When necessary the backups may be from other agencies or contractors. Any backup staff should receive the same training as the primary staff member. The plan should make provisions for the use of this backup staff during the time of a system outage.

In order to perform their jobs the team must have the needed resources available to them. The primary and most vital resource is a copy of the plan. Different team members may be issued different portions of the plan on a need to know basis for confidential information such as passwords, but the complete plan must be available to the team. At least one copy of the plan should be available from a location other than the TMC in paper format. This copy will be used by the team if they are not able to get access to the TMC.

Appropriate codes should be available within the plan. These include, if required, codes needed to activate the backup site and codes to move the termination points of the telecommunications lines. Codes of these types should be considered confidential information and should be included in plans for the appropriate person(s) only.

Another fundamental resource needed by the team is copies of the system backups. Again, these need to be able to be acquired without having access to the TMC facilities. Currency of the backup is a function of the goals of the organization as expressed in the plan.

Any dongles or other specialized equipment needed in order to run the systems must be available to the team. As was true with the other mentioned needed resources, this equipment must also be available to the team without access to the TMC.

The team should be supplied with personal communications equipment. Personal communications equipment such as cell phones will likely be standard equipment for these individuals. In that case, nothing special will need to be done during a system outage. Additional equipment may be activated during an outage such as satellite telephones.

Financial resources should also be available for team members during these periods. Quick purchases such as renting vehicles to move staff and critical office equipment that was not considered will need to be made. Living expenses at off-site locations is also possible, and staff members may not be able to put the money out with expectations of being reimbursed. The financial resources can take the form of credit cards, checks or cash.

A well produced plan is critical to the success of recovery and mitigation. But, a good plan is the beginning of the effort. The plan must be understood by all of the team members. It must be trained and practiced regularly by those that will have to execute it and their backups.

Training for the team should include both the implementation of the plan as well as the background under which the plan was developed. In this way, as unexpected issues arise they may be handled appropriately. Training includes processes, each team member's responsibility, intra- and inter-team coordination and communications, external communications and reporting procedures. Background information that should be communicated includes the agreed upon organizational mission and goals, scope of the plan and security requirements. In a case where a copy of the plan is not immediately available, the team should be able to begin the recovery process using the knowledge gained from periodic training.

Management

Management plays an important role during the planning and recovery processes. Strong commitment from management will ensure that a quality product is produced and continued support exists. Specific management concerns may be handled through the use of policies. With policies drafted, approved and communicated, management is able to ensure that pre-reviewed actions will be taken when specific types of outages or community-wide disasters occur. An example of this may be the suspension of toll collections during an evacuation event.

An executive sponsor or champion is vital in moving a recovery and mitigation effort forward. The champion should be high placed in the organization on both a formal and informal basis. The individual should be able to make necessary decisions, allocate resources and ask non-reports for help in the effort. The champion should report on the progress regularly to the most senior executive in the organization.

Management must also take appropriate actions to establish a recovery and mitigation team. The team life-cycle will initially require a large number of staff members relative to the future ongoing team. There are various methods of management structuring this team, but they must have access to the needed resources and have the authority to perform the needed tasks. The team will need to receive assistance from others in the organization that have been identified as subject matter experts. The team must have the backing from the management to get the expert's time as needed, given their other priorities

Initial contacts with other departments to set up institutional relationships should be achieved by senior level management. Contacts should be maintained with other transportation agencies, emergency management, law enforcement, fire and emergency medical services, public health, military and intelligence departments²⁵.

Documentation

Documented processes should include setting up methods for communicating with the point-of-contact in each of these entities in order to communicate pending issues from both the TMC and their organization. National Institute for Standards and Technology (NIST) suggests that information that is communicated may include:²⁶

- u Nature of the emergency that has occurred or is impending
- u Loss of life or injuries
- u Any known damage estimates
- u Response and recovery details

- u Where and when to convene for briefing or further response instructions
- u Instructions to prepare for relocation for estimated time period
- u Instructions to complete notifications using the call tree (if applicable)

During a system outage, management will function in a decision making role. No matter the extent of the planning that is undertaken, it is likely that all specifics of the occurrence will not have fully been anticipated. Immediate decision making is likely to be needed. The process should include the ability for people filling specific management roles to make decisions, as needed. It should also include a means of contacting management personnel to inform them about an outage, and a means to contact them during the outage. A location, during the recovery, for each included member of management should be identified in the plan, as well as a succession plan for the management staff.

The deliverable from the planning effort is the documentation. Fundamental examples of COOP documentation have been developed by the Federal Emergency Management Agency. This example documentation may be found at http://www.fema.gov/doc/government/coop/coop_plan_blank_template.doc with the related documentation available at http://www.fema.gov/doc/government/coop/coop_plan_template_instructions.doc . Even with these documents being fundamental, in order complete this plan, an understanding of the functions of the TMC and their relative prioritization is needed.

In preparing COOP documentation it is important to determine the high priority functions to restore, but it is just as important to determine which functions may be deferred until later. FPC 65 describes essential functions as those that “provide vital services, exercise civil authority, maintain the safety and well being of the general populace, and sustain the industrial/economic base in an emergency.”²⁷ These functions in a TMC may include specific device handling such as gates, along with pedestrian and vehicle mobility. Other functions may be of low enough priority that they may be deferred until the system outage has been rectified.

Recovery preparations should presume a worst case scenario. Worst case scenarios being contemplated when writing the recovery plan should consider situations, including:

- u The TMC being destroyed
- u Primary staffing of the team is not available to perform critical functions defined within the plan
- u All communications, both voice and data, are lost
- u Subsets of the overall plan can be used to recover from minor interruptions
- u Local transportation is not readily available

Rather than re-documenting information that may already be documented in other forms, other documentation may be referred to and stored with the recovery documentation. Documentation types that should be considered for inclusion are:

- u Contracts and Service Level Agreements (SLAs) with vendors
- u Software Licenses
- u System User Manuals

- u Security Manuals
- u Operating Procedures
- u Concept of Operations

Recovery plans must balance detail with flexibility. Detail is needed to enable less skilled personnel to execute the plan but may also reduce its scalability and adaptability.

In addition to the procedures and the team information, the documentation must also contain information on the network and the service providers. By documenting the network and service providers in detail, a long-term cold-site or the reconstruction of the TMC, if necessary, may be more easily built.

Network documentation should include procedures for managing the network infrastructure. During a period of severe system outages, the primary person that is responsible for managing the network may not be available for network management tasks. Documentation of these procedures will assure that other qualified staff members may perform standard network management tasks.

A detailed inventory of all hardware and software within the TMC should be documented. Documentation of hardware and software required for operations should include model and version information as well as any non-default configuration information. At a minimum the hardware inventoried should include, server and workstation systems, network hardware such as routers, switches and firewalls; data integrity configuration information including but not limited to, server and workstation computer systems including operating system and application software; data integrity hardware such as tape systems, printers, workstations, servers, hubs, switches, routers, and firewalls. Information for each item of hardware or software should include as applicable any specific models and level numbers, manufacturer and provider (including contact information), SLAs, operating system and IP address. Passwords for all items should also be included, but these should be documented in a fashion in which allows them to be secured. Additional information should include procedures for restarting, restoring or resetting the equipment, error handling and contacts for having the equipment fixed. Some of these may be covered with user manuals that may be stored with the recovery documentation.

A complete network diagram should be included or referred to and be stored with the recovery documentation. It should include static IP addresses, domain renewal, DNS translation, IP address/port forwarding, and routing tables.

Service providers, also known as service bureaus or applications service providers must also be addressed in a recovery plan. Importance to the mission and goals of the TMC that are provided by any service provider should be assessed. Depending upon their importance to required functions during periods of system outages, procedures should be put in place to bring the service provider back online in an appropriate manner. The documentation should include contact information for the organization, SLAs, and any passwords or keys needed for operations.

Once the documentation has been prepared and approved, ongoing updates are necessary. Some updates should be as the result of steps in other tasks, other from results of testing and still others from a periodic update effort. When projects are undertaken that result in system changes, that is changes to hardware, software, people, facilities or procedures; process within the organization

should ensure that the corresponding recovery documentation is also changed. This should be part of the change control procedures for any tasks that fit within these specifications.

All testing that is performed, both scenario and full testing, should be monitored by a third party that is present to take notes on methods to improve the recovery plan. These should be discussed along with team members' impressions in a review meeting at the end of the testing. Action items should be produced from the review to identify changes that are needed to update the plan.

Periodically the plan should be reviewed and updated with new information that may have changed and were not previously reflected in the documentation. Information that is likely to be in need of updating includes such items as team member's contact information and passwords. Changes to these types of data items happen periodically without tasks being initiated.

Management of changes to the recovery plan is often a complex exercise. It is imperative that all copies of the plan are up-to-date and accurate. Old copies should be destroyed with new copies replacing them. An inventory of the location of all copies of the plan will help in the effort of keeping the plan current. If softcopies of the plan are being used, CDs or memory sticks with serial numbers may be distributed, and then collected when new versions of the plan are being distributed. If the plan is only available on a network, team members should be asked to not make copies because they may become outdated. At least one printed copy of the plan should be maintained outside of the TMC so that it may be used immediately upon system outage without the need for a computer. This copy must also be kept up to date as changes are made.

Information within the recovery documentation is extremely sensitive and must be carefully controlled. No matter whether the documentation is stored on a network, delivered on electronic media or printed the documentation contains information that, in the wrong hands can cause significant issues for the TMC. Sensitive information such as the network layout, passwords and team member personal information may be kept separately. The TMC organization may elect not to distribute this information other than during an actual outage. Alternately the organization may selectively distribute sensitive information on a need-to-know basis. Excluding information that is considered by the organization to be sensitive, the remainder of the plan should be distributed on an as needed basis. Information that is not deemed to be sensitive may still cause the TMC problems if released. Any copies that are distributed should be carefully inventoried and only distributed as necessary.

Communications Infrastructure

Much of the complexity and sensitivity of recovery planning relates to communications. Communications has been identified by several TMCs that have experienced significant systems outages as the most critical issue in the outage. In the worst case, the community's communication infrastructure has been lost with the TMC being impacted along with the rest of the community. In a case of this type it is possible that a backup site will be of little help because the communications to the backup site is also down and/or all communications to field devices are down.

During periods of disaster there is a probability that the amount of communications capacity that needs to be replaced is not the amount that was needed pre-system outage. Rather there is the probability that there will be more than the normal number of users trying to access the systems. Users may include TMC personnel that do not normally access the system, personnel from other agencies and media usages.

As a part of inter-agency cooperation during times of community-wide disaster, common protocols should be developed and approved that will facilitate sharing between agencies. Data sharing may be facilitated in this way. It may also allow sharing command and control responsibilities of on-street instrumentation. Specific equipment may be delegated to different agencies for their use during these periods such as specific DMS' put under the control of the police in allowing them to communicate with the community.

Voice communications has been found to be critical during emergency situations as well. A backup technique that has been used during some outage situations is the use of cell phones. Cell towers and related infrastructure have been able to maintain connectivity at some times where all other voice communications has been down. A next step to take in a recovery effort for voice communications is the use of satellite phones. When using this type of equipment, special knowledge of use is required.

During any community-wide situation it is likely that, if the telephone lines remain active, problems will be found in getting access to the available telephone lines. The recovery plan and preparations should include requesting prioritization of voice communications during periods of community-wide emergencies for select people within the TMC. Priority in landline communications may be received through the Government Emergency Telecommunications Service (GETS) program. Information and applications for the GETS program may be found at <http://gets.ncs.gov/>. The equivalent program for cell phones is the Wireless Priority Service (WPS) program. Information and applications for the WPS program may be found at <http://wps.ncs.gov/>.

In the case of communications, as is true in other portions of the TMC recovery and mitigation planning, mitigation is a far better solution than having to recover. In the case of communications, mitigation may be gained through the use of multiple network paths. This may be gained through using redundancy capable technology when building the network. Alternatively, organizations establish multiple communications paths, each using a different technology. Some organizations have internet connectivity as a backup to the prime communications lines. Internet lines may be used for both data and voice communications. Other organizations maintain POTS lines to the central office which may be used for either data or voice.

Alternate Sites

Alternate site selection requires consideration and planning. Independent of the type of alternate backup site that will be used, licensing for all software should allow for testing of your disaster plan at an alternate site and, in case of a system outage, running the software at the alternate site. The costs of alternate sites are generally in direct relationship to the amount of time it will take to reestablish the systems. The possible types of alternate sites from most expensive to least expensive are:

- u Redundant Site
- u Hot Site
- u Cold Site
- u Reciprocal Agreement

Another type of alternate processing that should be considered is that of having the operations performed in a distributed manner. The people needing access to the system would gain access

using any internet service provider (ISP). They may use virtual private network (VPN) technology to keep the communications secure. In this way, the staff can operate from their own home or a hotel room. If the TMC building has an outage, to work in this way will require the servers to be located in a different installation than the TMC.

A redundant TMC is the most expensive alternative. Using this alternative, a second full TMC in a different location is established. Operations may be fully run from either of these two locations. When a piece of equipment is added or changed in the TMC, the same addition or change is made in the redundant TMC. Having redundant TMCs also provide the ability to perform full testing of any changes, and provide a fall-back position if a change does not work completely as expected.

One additional consideration should be made in deciding to use a redundant TMC. In order to get the maximum utilization from a redundant TMC it needs to be situated in a location where events that effect the primary location will not effect the redundant location. Financial regulators have told banks that the requirement is a separation of at least 100 miles.²⁸ It is more convenient and politically expedient to have the redundant TMC within the same community. When this happens, it is more likely that both the primary and redundant TMCs will be affected by the same events.

A hot site is normally a subscription service that is shared by a number of organizations. It contains all of the hardware that is necessary to run your TMC. Communications lines can be easily rerouted to the hot site when necessary. Periodic testing is allocated as part of the subscription fee. In order to reestablish your systems, all systems and data would be restored and the systems may begin running. Specific hot sites are often reserved on a first-come-first-serve basis. If someone is already using the hot site that is closest to you, you will be assigned to another hot site that is at another location assuming that one is available. Normally hot sites may be used for up to six weeks. By six weeks your organization must move to an alternate location which may be the original TMC, a new TMC or a cold site.

Cold sites are buildings that contain an infrastructure to which equipment may then be moved. Infrastructure may include items such as HVAC, PBX, raised floor, communications infrastructure, satellite and electric. A cold site may be located in a building or may be located in a truck or RV. An RV of this type would be equivalent to an RV communications center. If appropriate, this type of cold site may be used to establish a temporary TMC outside an inoperable TMC.

A final alternative is the use of a reciprocal agreement. With a reciprocal agreement the TMC has made an agreement with another agency to allow co-location and operations from their center in case of a system outage. This is not a suggested approach because most agencies find that they are forced to work with as little infrastructure as possible. This does not afford the extra infrastructure that is necessary to allow a second organization to also operate out of the same location.

If a reciprocal agreement is going to be used, it is imperative to have a memo of understanding (MOU) between the two organizations. The MOU should be approved by both organizations' legal departments before the arrangement begins. Included in the MOU should be provisions for both organizations to perform ongoing testing at the alternate site. It should include testing to evaluate the necessary extra processing and system compatibility with backup configurations. Testing should also prove that telecommunications are sufficient for both organizations and that security between the two organizations are compatible. As was true with the redundant TMC, if

the reciprocal site is too close to the original site there is the likelihood that both of the two organizations will have a system stoppage at the same time.

RISK MITIGATION

IBM suggests that there are several approaches that an organization may take in order to mitigate risk.²⁹ These include methods of keeping the systems simple and obvious. The mitigation techniques are

- u Simplify, consolidate, standardize and centralize infrastructure
- u Well documented and tested data center systems management procedures
- u Acquire systems management tools to monitor, prevent outages, automate diagnostics and recovery, and report to stakeholders
- u Make Business Continuity a strategic part of application and IT infrastructure Planning

Risk mitigation must be addressed by policy and planning, for each project which has effects on the TMC systems. When risk mitigation is planned, it should be considered against a standard of high availability. If the TMC can absorb some amount of system outages the mitigation strategy should be built on what currently exists in the infrastructure. If no downtime is acceptable for the organization, retrofitting a mitigation strategy is not appropriate. High availability must be built into the requirements and design of the initial TMC. It is not able to be effectively retrofitted into the systems after installation.

The TMC organization should perform an impact analysis on each system to determine the resources that should be applied to mitigating outage of the individual system. An impact analysis may be performed by quantifying the impact of a possible outage and multiplying that by the possibility of such an outage occurring. This measure may be used as a relative risk assessment between systems and may be used to justify and allocate resources to the highest impact systems.

Another basic risk analysis technique is to review systems for a single point of failure. Reviews should be conducted on all elements of the systems: hardware, software, people, facilities and procedures. A single point of failure is possible in any of these elements and should be eliminated, if possible.

Areas that should be considered for risk mitigation include the TMC infrastructure, physical security, logical security, technology, communications and related policies. In reviewing these areas and applying an impact analysis to each risk found, a mitigation approach may be developed.

Infrastructure includes those services and facilities that enable the TMC to operate on a day-to-day basis. Included are the building, electric power, HVAC and the like. NIST suggests that the following are common measures that may be taken to mitigate the infrastructure risk.³⁰

- u Appropriately sized uninterruptible power supplies (UPS) to provide short-term backup power to all system components (including environmental, safety controls, PBX and card access system)
- u Gasoline- or diesel-powered generators to provide long-term backup power
- u Air-conditioning systems with adequate excess capacity to permit failure of certain components, such as a compressor

- u Fire suppression systems
- u Fire and smoke detectors
- u Water sensors in the computer room ceiling and floor
- u Plastic tarps that may be unrolled over IT equipment to protect it from water damage
- u Heat-resistant and waterproof containers for backup media and vital non-electronic records
- u Emergency master system shutdown switch
- u Offsite storage of backup media, non-electronic records, and system documentation
- u Technical security controls, such as cryptographic key management and least-privilege access controls
- u Frequent, scheduled backups.

Some other infrastructure mitigations that may be considered include

- u Careful choosing of the TMC location
- u Building a hardened TMC

Closely aligned with the infrastructure risk mitigations are physical security risk mitigations. Physical security protects the critical infrastructure from destruction that may be due to mistakes made by personnel or vandalism.

Access to critical areas of the TMC, such as the server room, should be restricted on a need to have basis. This should be supported by an access device such as pass-card system. Critical areas should also be monitored by video surveillance. In this way, unauthorized people will not have access. All entrances should periodically be checked for signs of trespassing and forced entry.

Critical equipment should be positioned so that it is not visible from any windows or doors. This will provide the benefit that passersby will not know that this particular equipment exists and remains less of a temptation.

Less critical areas such as the TMC work areas should have enforced policies that prohibit eating and drinking. This will help prevent both inadvertent damage such as spilling drinks and food crumbs on equipment.

In addition to physical security mitigation, logical security mitigation should be taken. Logical security, also known as data security, has received a lot of visibility in the media recently. Terrorists may easily exploit weaknesses in data security. Even more basic than that, logical security help ensures that TMC personnel conduct themselves appropriately with automated equipment.

The most basic logical security is the issuance and management of system passwords. Having passwords in your system provides the ability to secure the TMC automated systems in an appropriate manner.

- u Review the password policy for appropriateness. Ensure it includes time frames requiring changes in passwords, requirements to make the password strong and not allowing generic IDs

- u Review access privileges to ensure that staff members have access that is at the level needed to perform their job.
- u All changes to access privileges should be reviewed
- u All access by personnel that have authority to override security rules, bypass security checks and parameters should be reviewed
- u Review access violation logs for trends, patterns or anomalies
- u Ensure that no one has used the security administrator's ID other than the security administrator.

Several additional basic mitigation efforts include restriction of people and programs from outside of your organization onto your network, and restriction of the places and programs that TMC personnel may access from the network. Firewalls and virus protection systems will help to enforce these concepts. Firewalls may be used to restrict other's access to the TMC network as well as restricting availability of the places to which TMC employees may navigate.

Knowing that, no matter the level of your protection there is always a possibility of viruses or spyware penetrating your system in some way, it is also a good mitigation to run both virus protection software and anti-spyware software on your equipment. With viruses and spyware constantly being updated, subscriptions to these services which provides update when available is a recommended procedure.

Technology may be used to mitigate risks, primarily to technology. There are technology solutions that allow for redundancy which may be selected as part of the TMC's technology solution. Depending upon the specific technology, many times it allows for internal redundancy such as a backup power supply or disk drive, or the ability for redundancy in the peripherals such as the communications lines.

A primary redundancy that should be explored within TMC systems should be in data storage. There are several technological solutions within data storage that may be explored including the use of redundant array of independent disks (RAID) and the use of storage area networks (SAN). Other solutions exist, but these give an idea of the types of redundancy available for disk storage.

RAID provides for redundancy of the disk drives themselves. Levels of RAID are from 0 to 5, each providing different levels of redundancy, requiring different hardware and software installation.

- u RAID 0 – No redundancy. This is the normal disk drive.
- u RAID 1 – Also called mirroring using two hard drives. The data is duplicated on both drives. If a disk drive fails, the system can move to the second drive.
- u RAID 2 – Not often used due to the high cost and complexity. With RAID 2, each individual bit within a byte is written to a different disk drive. Check bits are also written out. When read back in, the byte is verified and bits may be corrected if incorrect.
- u RAID 3 – Bytes are written to different disk drives with check bytes on another drive. When read back in, the bytes are verified and may be corrected if incorrect.

- u RAID 4 – Blocks of bytes are written to different disk drives with another drive being a check area. Again, with RAID 4, if invalid blocks are read back in, they may be corrected.
- u RAID 5 – Blocks of bytes and check data are written to different disk drives. With RAID 5 there is no specific drive that is used for the check information. This helps to cut down a bottleneck.

There are two other levels of RAID, 6 and 7, that are not as widely accepted but provide more of the same types of redundancy.

- u RAID 6 – Blocks of bytes and check data are written to different disk drives, as in RAID 5, but with RAID 6 there are two copies of the check data written. Again, in this version, no specific drive is designated for the check data.
- u RAID 7 – Rather than being a standard RAID, this is a proprietary version that is offered by only one vendor. It is a derivative of RAID 3 and RAID 4.

SAN is storage that resides on its own network and may connect to systems acting as local storage. The storage units will normally contain internal redundant components such as redundant power supplies.

In addition to storage, all major components should be reviewed for possibility of a mitigation strategy. These should include any mainframes, servers, firewalls and phone systems as well as any specialized and critical component within the TMC.

Mitigations within the communications infrastructures include both the ability to have multiple communications paths and penetration issues. These two issues encompass most of the probable issues that can befall a communications infrastructure in the TMC.

With multiple communications paths, the TMC is less likely to lose communications capabilities. When the communications paths use different technologies that are less likely to have a common component the likelihood is reduced even more.

In addition to the possible loss of communications lines, the other risk that may be mitigated is the penetration of the TMC computer network by unauthorized people. In order to help mitigate the risk of unauthorized access, penetration tests may be run on the TMC network. Penetration tests are normally run by people that are expert at this specific function. They attempt to hack into the TMC system, finding network exposures. Once found, these exposures can usually be easily rectified.

With TMC management considering recovery and redundancy an important issue that will be controlled, procedures and policies used daily can be put into place resulting in a smoother ongoing effort. These policies and procedures should include continued education of the staff in these issues, consideration of these issues in all systems development and practicing ongoing communications with other departments.

Education for staff of the TMC should, by policy or procedure, be an ongoing effort. This could be through the use of platforms such as classroom training, periodic newsletters and email notifications of serious issues that are occurring such as viruses.

Systems development methodology should include an analysis of the impact of the changes on recovery and mitigation strategies within the TMC. Remembering that systems include hard-

ware, software, people, facilities, and procedures; changes to any of these entities have the possibility of adversely affecting the recovery and mitigation strategy. A step within the process may be to have the process reviewed by the recovery and mitigation coordinator or committee for possible implications. An alternative method of review may be to have the person managing the change review possible implications for matches.

In order to build up the communications with other departments, policies and procedures should set standard types of and periods for interfaces with these departments. Communications may be such events as joint meetings, joint tests or having processes to work together on a daily basis with information that each may use from the other. An example of sharing information on a daily basis is having a direct telephone line to share information personally on an ongoing basis. By speaking together, rather than just passing data, a relationship will be set up between the people on the conversation. This relationship will be of help during a system outage.

Risk mitigation must extend to the recovery activities. In the event of a system outage the recovery activity becomes of paramount importance. Mitigation of risk during systems recovery will ensure a quicker system restoration.

Just as the first step on the planning process was to determine the mission and goal of the TMC in order to understand the extent of recovery and mitigation, performing business impact analysis (BIA) will specify the relative priorities of the components of the TMC for system restoration. In order to perform a valid BIA, participation will be needed from people at all levels of the TMC. A BIA will:³¹

- u identify functions critical to the TMC's survival
- u identify risks to those functions
- u rate (prioritize) risks by probability of occurrence and impact on the TMC
- u identify ways to avoid or mitigate identified risks
- u prioritize recommended avoidance and mitigation options

The best case would be to remove any risks that are within the TMC. Realistically this is not possible. Even if there is a possibility of removing risks, a cost/benefit analysis will indicate that many of the risks are of low enough in priority that they will not be eliminated. Rather, any outstanding risks should be lowered to an acceptable level.

NIST provides guidance in conducting such an analysis in NIST Special Publication 800-30, Risk Management Guide to Information Technology Systems.³² Within this publication a methodology is provided to determine the relative risk of individual system outage components.

A prime risk mitigation in the recovery effort is to ensure that the backups are appropriately conducted and handled. Backups are often needed outside of their use for system restoration. Any time that data is lost, through hardware or software failure, human error or natural disaster, backups are needed to restore the system to its previous state. It is important to provide appropriate backups to meet the goals of the TMC, but backing up too much data or too often will waste scarce resources. Retaining backups longer than needed may also subject the TMC to unnecessary liabilities. IBM suggests that legal counsel approve the organization's retention schedule.³³

Several methods of backups are available to use. Full or incremental backups may be used to backup the system. A full backup is a point-in-time copy of all files in storage. Full backups are normally much larger, requiring much more time to produce than an incremental backup.

An incremental backup will make a copy of changes that have been made since the last full or incremental backup that was made. When incremental backups are used, restoration requires first restoring the full backup, then following that each incremental backup is restored sequentially until all have been restored.

If data must be available until the exact time that the systems stopped, logging is also used in much the same way as an incremental backup is used. After the incremental backup has been made, logging begins for any changes that occur to the data. To restore the files, the full backup is restored, followed by each incremental, followed by the final log file.

The backup files, both full and incremental, must be stored outside of the TMC. If the TMC becomes uninhabitable, the backups may be damaged or inaccessible if they are left in the TMC. For the same reason, when logging is required, the logging should be accomplished at a site other than the TMC. Having backups and log files stored outside of the TMC may be accomplished through the use of electronic vaulting and remote journaling. In both cases, the files are created, and then may be stored off-site.

A final risk mitigation for file backup and restoration is testing of the restore. Restores must be tested often to ensure that backups are still usable in the current environment. At a minimum, testing of the backups should occur annually. Once the restore is completed, the system should be run to make sure that the restore not only completed correctly, but that the files are usable once restored.

With a valid backup available, the next important factor in which to mitigate risk is the alternate site. In order to mitigate the risk, care must be taken to pick a site that matches the organizational goals that have been determined. The most important of these goals that will be met by the alternate processing site is minimizing the amount of time that the TMC systems may be inoperative.

In order to mitigate risk during the recovery, when planning for use an alternate site it is important to assure that correct resources will be available at the alternate site. For each organization the necessary resources will be different. Available resources are needed to assure that the personnel can continue to do their work effectively at the alternate site.

As already discussed, the system backups will need to be available. In addition to the systems backup, other supporting applicable hardware and software should be available. These include hardware dongles and software keys, and operating manuals such as user and systems administrator's manuals. Normally used procedures and policy manuals will also need to be maintained at the alternate site.

A complete set of recovery manuals should be available for access. Confidential portions of the manuals such as contact lists and passwords must be available, although not made generally accessible. Any service level agreements, systems licenses and vendor maintenance agreements should also be available.

In planning for a system outage the existing SLAs with vendors should be reviewed. The SLAs should be reviewed to both ensure that they are in conformance with the goals and mission of the

TMC that are being supported, and expectations. If SLAs are not as expected a task to renegotiate the SLAs may be undertaken.

Essential functions should be identified, and the plan tuned to allocate resources in association with the relative priority. Using a relative prioritization within the plan will mitigate risks to the TMC ensuring higher priority items are handled with more priority and resources than lower priority items.

Appropriate logical and physical security at the alternate site is also required to mitigate risk during the recovery period. Logical security reviewed in light of the logical security that is in effect at the TMC. This may include both hardware and software such as virus protection, passwords and firewalls. Policies and procedures that relate to security should also be reviewed and considered strongly for use during the recovery period.

Physical security at the alternate site should be reviewed in advance in order to establish appropriate levels of physical security during a recovery. Access control, video surveillance and guards should be considered as possible security measures that may be used during the recovery period.

FUNDING AND APPROVALS FOR PLANNING

An investment in recovery and mitigation is an investment in security. It is an insurance policy in which it is hoped that you will never have to make a claim. It is an investment against the potential of a worst-case scenario.

Funding and approval of the recovery and mitigation planning project is an organizational commitment. A commitment to recovery and mitigation is based on an understanding that a system outage has significant impact on the services that the TMC provides. A commitment to recovery and mitigation is based on an understanding that recovery from a system outage is a significant undertaking. A commitment to recovery and mitigation is based on an understanding that the timing of a recovery from a system outage is of significant importance to the community.

Senior management must understand that there are many potential disasters that may cause a system outage. They must believe this and instruct the organization to mitigate the risk of having an outage and to plan for recovery of the systems in a manner that will be expedient and successful.

In order for a recovery and mitigation program to be successful senior management of the TMC must make a solid commitment to the project. They must prioritize the recovery and mitigation project high enough that it is not usurped. The project should also be included in the financial commitments of the TMC. Budgeting for an initial project as well as an ongoing commitment to funding support for the project is required.

Senior management's support for recovery and mitigation should translate into an organizational commitment and mindset towards recovery and mitigation. Each member of the TMC staff should recognize that as a portion of any change that is being contemplated, the recovery and mitigation implications must be analyzed. A committed TMC will both formally and informally do this analysis. As a formal part of the change process a task will be included to identify any implications. Informally each member of the TMC team should consider recovery and mitigation in every task that they undertake. Only with a true organizational commitment will the TMC have a suitable recovery and mitigation program.

Management within the TMC must budget for a recovery and mitigation program that includes those costs that are direct and those that are indirect. Direct costs include the staffing and consulting that is needed to produce the plan, any upgrades and additional hardware and software and services determined to be needed. Indirect costs include the time that personnel will spend doing their job due to additional processes. During the budgeting the direct and indirect costs will fall into the categories of personnel, capital and operating costs.

When budgeting for recovery and mitigation it is important to realize that there are also some possible savings to the organization that can occur. As part of the recovery and mitigation project, assets are inventoried. Using this inventory, it may be possible to negotiate agreements with suppliers with lower overall costs. Rather than paying maintenance on individual pieces of hardware and software, an asset inventory will allow the TMC to negotiate with suppliers based on a larger inventory of product. With software, an understanding of the number of each software product that is being used may be the basis for converting to usage based pricing. Ongoing support for software may be changed from workstation to server based, thus providing a more direct, less time-intensive support by the computer support staff.

In budgeting for recovery and mitigation, using a standard cost/benefit analysis will not normally be appropriate. Planning for recovery and mitigation is analogous to the purchase of an insurance policy. The benefits are soft, even if the plan for recovery is used for a significant system outage. There is little to no quantitative benefit that may be made from this type of plan. A well constructed plan should be considered a soft benefit, a benefit that is based on being more secure no matter the state of many factors outside of the TMC's control.

The goal of your recovery and mitigation plan is to allow system downtime to be within acceptable ranges, ranges that will allow the TMC to still make its goals and provide needed support to the community. Budgeting for the function should be set to an amount that will provide for this level of support.

Recovery and mitigation should be budgeted for an initial project to establish the plan and then following years for ongoing testing and updates. The costs that should be budgeted include direct and indirect costs. Direct costs are those that will be directly attributed to the recovery and mitigation project such as an additional staff member to manage the project, consulting services or hardware upgrades. Indirect costs are those that will not specifically be attributable to the project such as the time that the senior TMC staff members will be spending with the team to explain processes, policies and issues.

CONTINUITY OF OPERATIONS

Continuity of Operations, also known as COOP, includes recovery and redundancy from a complete systems point of view and not just from a computer hardware and software point of view. COOP speaks to continuity of operations in terms of allowing for high availability, continuous operations, and disaster recovery.³⁴

The federal government officially considers COOP a “good business practice” due to the changing threats of acts of nature, accidents, technological emergencies and military or terrorist attack-related incidents.³⁵ Unfortunately, even though there are many reasons that COOP is important to our TMCs, IBM found that it is usually an afterthought.³⁶

The Freeway Management and Operations Handbook³⁷ defines the objectives of COOP as:

- u Ensuring the continuous performance of an agency's essential functions/operations during an emergency.
- u Protecting essential facilities, equipment, records, and other assets.
- u Reducing or mitigating disruptions to operations.
- u Reducing the loss of life, minimizing damage and losses.
- u Achieving a timely and orderly recovery from an emergency and resumption of full service to customers.

The handbook describes the elements of COOP much as what has been described as being part of recovery and mitigation plans:

- u Plans and Procedures
- u Identification of Essential Functions
- u Delegations of Authority
- u Orders of Succession for Key Positions
- u Alternate Facilities
- u Interoperable Communications
- u Vital Records and Databases
- u Tests, Training, and Exercises

As a rule-of-thumb when planning for COOP, an objective of the planning is to be able to continue the operations in an alternate facility for 30 days. By the end of the 30 day period it is expected that either the TMC will be able to move back into the original facility or other arrangements have been made.

The plan for a COOP is closely aligned to that recommended for recovery and mitigation. The steps for implementation COOP is described by IBM as equivalent to that of recovery and mitigation as:³⁸

- u Simplify, consolidate, standardize and centralize infrastructure
- u Well documented and tested data center systems management procedures
- u Acquire systems management tools to monitor, prevent outages, automate diagnostics and recovery, and report to stakeholders
- u Make Business Continuity a strategic part of application and IT Infrastructure Planning

IBM has described various levels of COOP.³⁹ These same levels are applicable to levels of recovery that may be considered by the TMC. As described previously, the goals and objectives of the TMC should match the tier of availability that is listed below.

- u NO RESTORATION
 - Tier 0 – No Backup
- u BACKUP/RESTORE
 - Tier 1 - "Cold Site" – (recovery time in days) Restore from Tape

- Tier 2 - "Remote warm site" – (recovery time in 1 day) Hot Site, restore from tape
 - Tier 3 - "Remote tape vault" – (recovery time in 12-16 hours) Electronic Vaulting
- u RAPID DATA RECOVERY
 - Tier 4 - "Point in Time Copy" – (recovery time in 6-10 hours) Point in time disk copy
 - Tier 5 - "Database Replication" – (recovery time in 3-6 hours) Software mirroring (transaction integrity)
 - Tier 6 - "Hot-Standby" – (recovery time in 1-4 hours) Storage mirroring (with or without automation)
 - u CONTINUOUS AVAILABILITY
 - Tier 7 - "Hot-Hot" – (recovery time in <1 hour) Site mirroring with automated recovery

TESTING OF THE PLAN

Planning for recovery is a prime mitigation for troubles during times of system outage. Once the plan is completed, the most significant mitigation that is available is testing. Testing of the plan allows for validation of the logic that has been developed for the TMC. It allows the assurance that during a system outage that a restore will be accomplished in an acceptable manner.

Testing also acts as an additional vehicle for training the TMC staff in recovery and mitigation and the TMC's approach. It ensures that the people that are involved in the testing effort will have exposure to the methods that are being used to rectify a system outage. Questions may be asked and answered during and after the test to clarify that the participant understands of the process.

The testing may also be another opportunity to give participants from various departments the ability to interact. Interaction of this type will aid in future interaction during times of true system outages.

Testing of the plan should consist of both scenario testing and full testing. These each have important objectives and are needed to be accomplished periodically. Each of these types of testing may be accomplished with either TMC personnel only or may be a part of a much larger, inter-agency test.

The scenario testing, also known as desk testing, may be held in a conference room. In this form of testing staff members from different areas within the organization will represent their function. Using the plan, different scenarios of system outage are logically walked through with discussions held covering the specific process used for that scenario. The intention of scenario testing is to find errors in the plan where specific scenarios have not been taken into account while developing the plan. Some possible examples of scenarios are

- u Full electrical outage in the TMC
- u Full electrical outage in the community
- u Full electrical and communications outage in the community

- u Full electrical and communications outage in the community caused by a major fire

Full testing entails staging of a simulated system outage. In planning, a test scenario must be chosen for use. Minor staging tests may be accomplished periodically which test individual components such as switching over to emergency power to prove that these devices still work. Full test scenarios should begin with a straight forward concept such as recovery from a system outage that is caused by a loss of electricity localized to the TMC. These scenarios may progress through ones such as a system outage at the TMC that is caused by a generalized communications outage throughout the community. These may proceed to very sophisticated scenarios such as the loss of both the TMC and key personnel due to two concurrent issues. The scenarios may be localized to the TMC only or may be a community wide emergency where testing is simultaneously performed by the TMC and other emergency agencies within the community.

Regardless of the type of test that is being undertaken the testing should be monitored by a third-party. It is the responsibility of this person to keep notes on errors and issues that have been encountered during the test. They should have a complete test plan and participants in the test should notify them as tasks are complete. A report of the findings of the test monitor should be provided to the testing team.

The testing team should gather as soon as possible after the test has been completed. In this meeting every member of the team should bring forward any testing issues that they found. Also, any impressions that the members have about methods to make the test better should also be brought up. The deliverable from this review meeting is a set of action items that need to be completed to correct errors that have been found and to improve the overall plan.

ONGOING SUPPORT FOR THE PLAN

The environment of the TMC is changing constantly. Many of the changes are outside of our control but still effect the TMC operations. Other changes are within the TMC's control. Any changes whether under the TMC's control or not must be considered for their implications to recovery and mitigation.

The changes that must be considered should be those that affect the hardware, software, facilities, people or procedures. Changes affect any part of the system. Some examples of changes that may affect the system include:

- u Promotion of employee
- u Employee that moves their residence
- u Requirement to add area code to dialing local telephone number
- u Vendor business sold
- u Upgraded network
- u Changes to a law

Ongoing upgrades to the recovery and mitigation plan should be handled as a part of the change procedure for system elements. Procedures should be in place that monitors any changes to systems. This function is often handled by a Configuration Control Board (CCB) which is made up of representatives of each organization within the TMC. Each person on the CCB represents the interest of their organization and determines if the change will present problems within their

area. Personnel responsible for recovery and mitigation should be included in the CCB to determine changes that affect these efforts. Changes that require changes to recovery and mitigation will create action items for the appropriate person to update the plan.

Additionally, the complete plan should be periodically reviewed for changes that have not been found in any other manner. The periodic review should be at least once per year. It may be appropriate to review the complete plan before each test cycle, which should be more often than the once per year suggested.

Whenever the plan is changed, the changes must be versioned, or reflected in all documentation in all locations. The recovery and mitigation coordinator must make certain that all copies of the documentation that have been distributed have been updated to include the new changes.

Funding for ongoing support should be included in the budget each year. Depending upon the TMC organization, this may include one or more extra staff members that will schedule and coordinate training and testing, update the documentation, represent the interests of recovery and mitigation in the CCB and distribute any changes to the holders of the documentation. Additional money should be budgeted for, as applicable, items such as

- u alternate sites
- u storage of backups
- u periodic testing
- u periodic training and education
- u equipment needed for recovery and mitigation

²⁰ www.fema.gov/onsc/docs/coop_plan_blank_template.doc

²¹ Federal Preparedness Circular (FPC 65), FEMA, July 26, 1999, www.fas.org/irp/offdocs/pdd/fpc-65.htm

²² Washington Technology Continuity of Operations and Disaster Recovery Forum, February 15, 2006

²³ Warrick, Cathy, et al, *IBM TotalStorage Business Continuity Solution Guide*, International Business Machines Corporation, 2005, ISBN 0738491136

²⁴ Info Tech Research Group, *Building a Comprehensive disaster Recovery Plan*, 2005 (ISBN 0-9730108-7-8) (and workbook)

²⁵ "The FHWA's Role in Enhancing Surface Transportation Security" (Interview with Vince Pearce), Newsletter of the ITS Cooperative Deployment Network, April 22, 2003, http://www.nawgits.com/icdn/pearce_security.html

²⁶ Swanson, Marianne, et al, *Contingency Planning Guide for Information Technology Systems*, NIST Special Publication 800-34, June 2002

²⁷ www.fas.org/irp/offdocs/pdd/fpc-65.htm

²⁸ Crosman, Penny Lunt, "A Watertight Plan", September 1, 2005,

<http://www.itarchitect.com/shared/printableArticle.jhtml?articleID=169400810>

²⁹ Warrick, Cathy, et al, *IBM TotalStorage Business Continuity Solution Guide*, International Business Machines Corporation, 2005, ISBN 0738491136

³⁰ Swanson, Marianne, et al, *Contingency Planning Guide for Information Technology Systems*, NIST Special Publication 800-34, June 2002

³¹ "What is Business Continuity Planning?: How does it Differ from Disaster Recovery Planning?", *Disaster Recovery Journal*, Volume 15, Issue 1, Winter 2002

³² <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>

³³ Warrick, Cathy, et al, *IBM TotalStorage Business Continuity Solution Guide*, International Business Machines Corporation, 2005, ISBN 0738491136

³⁴ Warrick, Cathy, et al, *IBM TotalStorage Business Continuity Solution Overview*, International Business Machines Corporation, 2005, ISBN 0738491152

³⁵ Federal Preparedness Circular (FPC 65), FEMA, July 26, 1999, www.fas.org/irp/offdocs/pdd/fpc-65.htm

³⁶ Warrick, Cathy, et al, *IBM TotalStorage Business Continuity Solution Guide*, International Business Machines Corporation, 2005, ISBN 0738491136

³⁷ *Freeway Management and Operations Handbook- Chapter 12: Freeway Management During Emergencies and Evacuations*

³⁸ Warrick, Cathy, et al, *IBM TotalStorage Business Continuity Solution Guide*, International Business Machines Corporation, 2005, ISBN 0738491113

³⁹ Warrick, Cathy, et al, *IBM TotalStorage Business Continuity Solution Overview*, International Business Machines Corporation, 2005, ISBN 0738491152

4

RECOVERY AND MITIGATION POLICIES

Chapter 4 Purpose:

To review policy implications of recovery and mitigation. This chapter will suggest possible policies to be implemented in order to reduce risks associated with mitigation strategies such as high availability as well as risks associated with recovery activities. Issues associated with returning the TMC to normal operating conditions will also be addressed.

Chapter 4 Key Message:

- u As part of a recovery initiative, specific policies may lower risk.
- u Returning to normal operations must be planned and executed in much the same manner as was used to move to an emergency condition.

POLICY ISSUES

“How important is it for your TMC to be able to mitigate the impacts and recover from a disaster?” In reality, asking how critical is “critical” is the central question for policy makers who must set priorities for protecting and restoring public resources, such as a TMC. There are a number of factors that go into the development of public policy, including many intangibles, however, that are truly beyond the scope of this document.

Decision making under emergency situations is difficult enough, but guiding policies can do much to help simplify this process. These policies should be developed based on the specific requirements of the TMC operating agency and other stakeholders. Requirements that will drive Disaster Recovery and Mitigation (DRM) specific policy issues include the following:⁴⁰

- u Identify management authority needed for effective operations at all levels having emergency responsibilities
- u Identify circumstances under which management authority would be exercised
- u Document the necessary management authority at all point where emergency actions may be required
- u Delineate limits of individual authority and accountability
- u Determine the successors and predetermined delegation authority, termination of the delegation
- u Personnel get proper training for emergency duties
- u Specify responsibility and authority of personnel that will be members of overall DOT teams during emergency.

- u Who makes the decision to go into a recovery mode?

Most will agree that it is not possible to plan for every potential event, but how much planning and preparation is “good enough”? One way to answer this question is by defining what metrics of success the DRM plan should address. The following are some key metrics of success recommended in relevant guidelines:⁴¹

- u What is the required uptime for the TMC that is expected on a weekly, monthly, and annual basis?
- u What is the TMC’s required system response time that is expected, even during a recovery?
- u What is the TMC’s required number of IT transactions per minute, hour, and day during recovery situations?
- u What is the TMC’s Recovery Time Objective (RTO)? Given the RTO, what amount of data can the recovery recreate?
- u What is the TMC’s budget for recovery and mitigation? Who pays for that budget? Is the budget a part of a larger project?

The policies of the TMC as an operating agency provides both the motivation and authorization for implementation of the actions and procedures needed to mitigate the potential impact of a disaster and recover from such as disaster. In this section, policy issues are examined for the following general categories:

- u Communications
- u Decision making
- u Prioritization of needs
- u Plan maintenance & updates
- u Risk mitigation

In the last section of this chapter, policy issues surrounding the return to normal operations are examined.

Internal Communication Policies

There is no question that communication is central to the TMC function, so it will come as no surprise that communication is critical to managing the recovery process after a disaster. Policies governing internal communications within the TMC operating agency are important for communicating what the DRM plan is, what is expected of each participant, and also to govern the communication priorities while in the recovery process and whenever operating under extraordinary circumstances.

The National Institute of Standards and Technology (NIST) guidelines for contingency planning for IT systems provide the following recommendations:⁴²

Staff and management need to know what has occurred, the status of the situation, what actions they should take, and who is in charge of the situation. One person

or team should be responsible for internal communication. This person should have access to the organization's senior leadership. In addition, the organization should be prepared to use multiple communication methods such as voicemail, e-mail, flyers, or Web site announcements. Clear and frequent communications from senior executives to all personnel, interconnected POCs, and end users is necessary after a disruption to assist calming internal anxiousness, worry, and answering general questions.

Senior management has both the responsibility and the authority to prepare for and implement the DRM plan. Internal communication policies must support the two-way flow of information between front-line operations and senior management.⁴³ Internal communication policies should cover as many foreseeable situations as possible, including as a minimum, the following:

- u Function of team in internal communications – what each person or position's role is and what is expected of them during the recovery process
- u Notification/Activation communications – who or what event declares a state of emergency that requires activation of the DRM plan
- u Quality of information being communicated – in the face of poor quality or conflicting information; how to determine what information should govern
- u Timing of communications – how often updates must be disseminated; research has strongly emphasized that, under emergency conditions, speed is of the essence⁴⁴
- u Pre-established modes and protocols for internal communications – what governs from the standard operating procedures (SOP) and what changes under emergency conditions
- u Types of information to be communicated – minimum and desirable levels of information
- u Communications to keep senior management and staff informed – predetermined distribution lists, based on severity and type of emergency

Recognize that in the excitement and stress of a major event, clarity of communication will likely suffer without specific guidelines. Recommended templates for notification information may include:⁴⁵

- u Nature of the incident that has occurred or is impending
- u Loss of life or injuries
- u Any known damage estimates
- u Response and recovery details
- u Where and when to convene for briefing or further response instructions
- u Instructions to prepare for relocation for estimated time period
- u Instructions to complete notifications using the call tree (if applicable)

Even the best laid plans can run into problems when a key resource becomes unavailable. For example, policies and notification strategies should define procedures to be followed in the event that specific personnel cannot be contacted. Notification procedures should be documented clearly in a contingency plan.⁴⁶

External Communications Policies

These days, no TMC operates as an island. External communications, with stakeholders outside the TMC operating agency, are critical to meeting overall TMC objectives, especially during times of crisis. An assessment of the lessons learned following the Northeast power blackout in 2003 stressed the importance of having pre-established modes and protocols of communication – telephone, fax, or Internet – for agencies to contact each other during emergencies, with particular attention paid to ensuring redundancy in the methods and systems for communication.⁴⁷

In many cases, the standard operating procedures for the TMC will already provide procedures and protocols for communicating with external stakeholders. The first policy question then is, “What changes are required under an emergency situation?” It may be necessary to authorize additional people to initiate and maintain external communications due to changes that the outage is imposing on the TMC’s capabilities. Therefore, policies governing the authorizations and communication procedures should include the following as a minimum:

- u Authority for communications with other governmental agencies – who, what, when and how often
- u Authority and process for communications with the private sector– who, what, when and how often
- u Authority and process for communications with the media – often referred to as a “double edged sword”, the media can be a friend that helps disseminate information, or a foe that raises criticism of the TMC performance under crisis. Governing policies must be established for who, what, and when information can be passed to the media.

Decision Making Policies for Outage Management

One of the key lessons learned by emergency responders dealing with highway incident management is the importance of a well defined hierarchy of decision making authority to manage on-scene activities. The decision making policy is designed to minimize confusion when responding to incidents and reinforce the chain of command. The same approach is recommended for emergency events affecting the TMC. As the emergency operations plan is developed consideration must be given to the process by which the plan is put into action.

The following policy issues related to decision making have been identified in the research:⁴⁸

- u Identify management authority needed for effective operations at all levels having emergency responsibilities
- u Identify circumstances under which the management authority would be exercised
- u Document the necessary management authority at all point where emergency actions may be required
- u Delineate limits of individual authority and accountability
- u Determine the successors and predetermined delegation of management authority, termination of the delegation
- u Personnel get proper training for emergency duties

- u Specify responsibility and authority of personnel that will be members of overall DOT teams during emergency.
- u Who makes the decision to go into a recovery mode?

In order for the decision making guidelines to address these issues, the following types of policies should be established:

- u Criteria for making a decision to go into emergency operations – in addition to designating which person or position has the authority to make the decision, the criteria that must be met should clearly articulated so in case the designated person is unavailable, his or her successor has the proper guidance.
- u Coordination with all those that need the information – this is more than just a “good idea”; it is so critical that policies must be in place to require such coordination. When the decision has been made to go into emergency operations, everyone should know about it, both internal and external stakeholders.
- u Service Level Agreement requirements for suppliers – suppliers such as power companies, network service providers, telephone, etc., must be notified that the TMC (and its critical infrastructure) is a critical public safety system that requires restoration of service at the same priority as other similar public safety institutions, such as hospitals, emergency responders, water and sewer supply, etc.

Policies for Setting Priority by Length of Outage

The TMC must be able to respond to extended outages or operation under emergency operations. Depending on the time span or the severity of the interruption, significant consequences, including the viability and relevance of the TMC’s function depend on the ability of management to quickly re-establish critical TMC functions. Usually, the TMC has many functions, some of which have required years to create and establish. In the case of an outage or emergency, only basic functions can be re-established within a few hours or days.⁴⁹ If the outage or emergency condition lasts for more than a few days, these basic TMC functions may not be sufficient to handle public safety needs and stakeholder expectations for the longer term. Therefore, additional policies are required for setting priorities for restoration of various functions by length of outage.

As the duration of a critical outage increases, policies should dictate recovery priorities based on the specifics of the emergency and each TMC function.

- u Variables to consider in deciding the recovery time objectives:
 - Is the recovery to be accomplished on-site or is relocation to a backup TMC required? Relocation requires higher priorities on basic shelter, power, and communication needs.
 - Are major field infrastructure elements involved, such as center to field communications? If field elements and external networks are largely intact, greater priority can be placed on TMC functions.
 - Has the emergency impacted the availability of key personnel? If so, identification of personnel replacements and retraining will take priority over hardware and software restoration.

- u Determination of recovery time objective categories by function:
 - Surveillance – a “blind” TMC is of little use in meeting its primary objective; therefore restoration of surveillance should be given a high priority. However, this mainly applies to video surveillance, center to field voice communication and possibly environmental conditions monitoring. Traffic flow surveillance is less important during the initial stages of an outage, but is a good example of a function whose priority for restoration should increase with longer duration outages.
 - Dispatch Response – smaller systems, with say less than 8 – 10 vehicles dispatched by the TMC, can typically manage (albeit with reduced efficiency) for a short time without the TMC dispatch function. Assuming radio communication between vehicles is available, coordination and dispatch can be handled by the drivers in the field. Medium to large systems (>10 units controlled by a dispatcher) will require a higher priority for restoration of the dispatch function.
 - Travel management – obviously, this is typically a high priority function for the TMC. All enabling services for travel management, surveillance, communications, TMC software, etc., should be considered a high priority for restoration following an outage. Individual sub-systems of travel management, such as VMS, HAR, traffic signal control, ramp metering, will have differing priorities based on the travel management effectiveness in each local situation. These subsystems should also be prioritized by critical travel corridors
 - Traveler information dissemination – depending on the nature of the outage, information dissemination to the traveling public can have more or less importance. In the case of an area or region wide natural disaster or similar emergency, traveler information should be a very high priority. In the case of an outage limited to the TMC, traveler information may take a lower priority than the reestablishment of other critical functions, such as surveillance or travel management. If the duration of an outage extends more than a few days, without restoration of traveler information, consider presenting a regular status report, via press conferences or briefings, as a substitute for the automated information dissemination.

Policies for Setting Priority for DRM Planning

DRM planning should be driven by standing policies that clearly dictate the reasons for the plan, the commitment of operating agency and, probably most importantly, the funding for the planning process.

- u Reasons for recovery and mitigation planning – probability of disaster is real and there is a need for business continuity for these critical public safety systems
- u Management’s commitment to the planning process – commitment to the DRM planning process is as important as the commitment to having a TMC in the first place
- u How the planning fits into the normal operations and budgeting cycles – as a matter of policy, the funding for the initial DRM plan should be a part of the ongoing TMC operations budget, so that it can be more easily incorporated as an ongoing process

Remember that disaster recovery planning is not just an IT project. DRM planning for the TMC is far reaching and must be considered an agency-wide project.⁵⁰

Policies for Ongoing Plan Maintenance & Updates

One of the goals of this document is to outline the reasons that disaster recovery and mitigation planning is important to the long term efficacy of the TMC. Of equal importance is that these DRM planning activities should not be considered a one-time event, but rather as part of the TMC program for overall preparedness. As with the base policies that govern the initial DRM plan, policies are required to govern ongoing updates and maintenance of the plan in each of the same categories as above.

- u Reasons for ongoing planning – the risks to a TMC, as well as the probability of occurrence can change over time, requiring updates to the plan.
- u Management’s commitment to ongoing planning – the physical infrastructure of the TMC and its field components all require maintenance; so does the DRM plan for business continuity.
- u How ongoing planning fits into normal operations and budget cycles – consider a policy that requires funding of the DRM planning process as a program, with periodic updates, rather than as a one-time project

Succession Planning Policy

As unpleasant as it may be, planning for the replacement, or succession, of key personnel following a disaster is critical to the continuity of the TMC. Orders of succession for key positions and titles within the agency, including the conditions under which succession will take place and method of notification, should be spelled out in the DRM plan.⁵¹ It is recommended that successors be geographically dispersed and that they receive appropriate training and orientation.⁵² The key policy elements that are required to support succession:

- u Establish lines of succession – two or more people deep is recommended
- u Ensure that lines of succession are applicable to times of emergency operation – list the criteria for implementation
- u Train backups in the work and decision making of the prime position – initial and follow-up training and orientation

Risk Mitigation Policy

Previous sections have identified risk assessment techniques and mitigation approaches. From a policy standpoint, the important consideration is the acknowledgement of each risk to the TMC and its related staff and infrastructure and the acceptance of those risks with or without mitigation and/or recovery steps.

In addition to the risks that may apply to the TMC itself, that may be risks that are exacerbated by an outage of the TMC. For example, there may be specific risks to the public if a service, such as incident detection and response, is down for a certain period.⁵³

Risk mitigation policy should govern more than just external threats. The standardization of various system components, as an agency policy, can mitigate certain risks. System recovery

may be expedited if hardware, software, and peripherals are standardized throughout the distributed system. Recovery costs may be reduced because standard configurations may be designated and resources may be shared. Standardized components also reduce system maintenance across the organization.⁵⁴

Risk mitigation policies should cover the following elements:

- u Personnel succession planning and documentation
- u Back-out planning and execution for system upgrades
- u Standard hardware
- u Standard software
- u Standard communications

RETURNING TO NORMAL CONDITIONS

It should be assumed that any emergency conditions requiring the implementation of a recovery plan will be temporary. Therefore the planning and preparation for a recovery and return to normal operations will begin the day following the emergency. During recovery, or reconstitution of the TMC, agencies work to re-establish safe, reliable, and secure transportation on the region's roads despite whatever damage may have occurred.⁵⁵

Planning for Returning to the TMC

In the reconstitution phase, recovery activities are terminated and normal operations are transferred back to the organization's facility. Policies governing the reconstitution phase should specify teams' responsible for restoring or replacing both the site and the IT system. The following major activities occur in this phase:⁵⁶

- u Ensuring adequate infrastructure support, such as electric power, water, telecommunications, security, environmental controls, office equipment, and supplies
- u Installing system hardware, software, and firmware. This activity should include detailed restoration procedures similar to those followed in the Recovery Phase
- u Establishing connectivity and interfaces with network components and external systems
- u Testing system operations to ensure full functionality
- u Backing up operational data on the contingency system and uploading to restored system
- u Shutting down the contingency system
- u Terminating contingency operations
- u Securing, removing, and/or relocating all sensitive materials at the contingency site
- u Arranging for recovery personnel to return to the original facility.

Timing of the Return to the TMC

Unlike the emergency condition that warranted the implementation of the DRM plan and transfer to temporary facilities, the return process should take advantage of the calmer atmosphere to make sure that everything (or most everything) is ready for the reconstitution of the permanent.

The timing for returning to the TMC should be structured as any major project, with the identification of critical path elements and tracking of action items.

Once the original or new site is restored to the level that it can support the IT system and its normal processes, the system may be restored back to the original or to the new site. Until the primary system is restored and tested, the contingency system should continue to be operated.⁵⁷ Critical assessments will be required of the following:

- u Availability of redundant site
- u Availability of reciprocal site
- u Availability of hot site
- u Availability of cold site

Implications of Being at an Alternate Site

Experience has shown that there can be many implications to both agency operations and personnel during the relocation to an alternate TMC site. During a serious situation, addressing personnel and family matters often takes priority over resuming business. Planning for such matters may involve pre-identification of temporary housing, workspace, and staffing.⁵⁸

- u Location relative to other departments – this may affect response times and the availability of incident response and maintenance resources
- u Personnel family issues – may affect absenteeism, morale, and efficiency
- u Additional costs of working from alternate site – affecting both agency and personnel budgets, this will have greater affect over the long term

⁴⁰ Federal Preparedness Circular (FPC 65), FEMA, July 26, 1999, www.fas.org/irp/offdocs/pdd/fpc-65.htm

⁴¹ Warrick, Cathy, et al, *IBM TotalStorage Business Continuity Solution Overview*, International Business Machines Corporation, 2005, ISBN 0738491152

⁴² Swanson, Marianne, et al, *Contingency Planning Guide for Information Technology Systems*, NIST Special Publication 800-34, June 2002

⁴³ Info Tech Research Group, *Building a Comprehensive disaster Recovery Plan*, 2005 (ISBN 0-9730108-7-8) (and workbook)

⁴⁴ Info Tech Research Group, *Building a Comprehensive disaster Recovery Plan*, 2005 (ISBN 0-9730108-7-8) (and workbook)

⁴⁵ Warrick, Cathy, et al, *IBM TotalStorage Business Continuity Solution Guide*, International Business Machines Corporation, 2005, ISBN 0738491136

⁴⁶ Swanson, Marianne, et al, *Contingency Planning Guide for Information Technology Systems*, NIST Special Publication 800-34, June 2002

⁴⁷ DeBlasio, Allan, et al, *Effects of Catastrophic Events on Transportation System Management and Operations: August 2003 Northeast Blackout, Great Lakes Region (Final Report)*, DOT-VNTSC-FHWA-04-04#, May 2004

⁴⁸ Federal Preparedness Circular (FPC 65), FEMA, July 26, 1999, www.fas.org/irp/offdocs/pdd/fpc-65.htm

⁴⁹ Warrick, Cathy, et al, *IBM TotalStorage Business Continuity Solution Guide*, International Business Machines Corporation, 2005, ISBN 0738491136

⁵⁰ Info Tech Research Group, *Building a Comprehensive Disaster Recovery Plan*, 2005 (ISBN 0-9730108-7-8) (and workbook)

⁵¹ *FREEWAY MANAGEMENT AND OPERATIONS HANDBOOK, FINAL REPORT*, Federal Highway Administration, September 2003

⁵² *Washington Technology Continuity of Operations and Disaster Recovery Forum*, February 15, 2006.

⁵³ Info Tech Research Group, *Building a Comprehensive disaster Recovery Plan*, 2005 (ISBN 0-9730108-7-8) (and workbook)

⁵⁴ Swanson, Marianne, et al, *Contingency Planning Guide for Information Technology Systems*, NIST Special Publication 800-34 , June 2002

⁵⁵ Pearce, Vince, “Securing the Roads”, <http://security.transportation.org/sites/security/docs/TTISecurityArticle.pdf>

⁵⁶ Swanson, Marianne, et al, *Contingency Planning Guide for Information Technology Systems*, NIST Special Publication 800-34 , June 2002

⁵⁷ Warrick, Cathy, et al, *IBM TotalStorage Business Continuity Solution Guide*, International Business Machines Corporation, 2005, ISBN 0738491136

⁵⁸ Swanson, Marianne, et al, *Contingency Planning Guide for Information Technology Systems*, NIST Special Publication 800-34 , June 2002

5

TYPES AND CAUSES OF SYSTEM OUTAGES AND RELATED RECOVERY AND MITIGATION

Chapter 5 Purpose:

To review the causes of system stoppage in detail and discuss what may be done in order to mitigate appropriate ones. Because all possible combinations of causes can not be anticipated, this chapter's discussion is based on the possible effects of the system outages.

Chapter 5 Key Message:

- u It is not possible to plan for all of the causes of system outages
- u The effects of the outages may be planned for and mitigated as appropriate

MITIGATION

The best way to handle a system outage is to prevent it from happening at all. Mitigation of system outages is an important step the TMCs should take in order to prevent system outages from occurring so as to never have to recover systems. There is no means to identify every possible cause of system outage and thus it is not feasible to avoid every possible type of system outage, even if all the resources that are requested were allocated to this task.

In order to determine the amount of resources that should be allocated to possible mitigations, it is a good idea to perform an impact analysis, which is also called a Business Impact Analysis. The analysis defines the functions that are critical to the TMC. Once these functions have been defined, the analysis will proceed to define the risk associated with the loss of each critical function. Using a quantification of these two values, the analysis then will prioritize the functions to which resources should be allocated to mitigate a possible outage.⁵⁹

A system outage may be caused by any component of the system becoming unavailable. These include hardware, software, people, facilities, or procedures. The loss of any one of these will create some level of system outage.

LOSS OF INFRASTRUCTURE

In reviewing the catastrophic events of September 11, 2001, the Port Authority of New York and New Jersey indicated that, "The Port Authority has always understood the dependant relationships between its transportation network and its building facilities, from an operations perspective."⁶⁰

Communities depend upon their TMC. The infrastructure is of primary importance to keep the TMC and its systems operational.

Loss of infrastructure may be caused by losing any of the basic facilities or services needed for day to day activities within the TMC. The most obvious is the building itself. If the building is not available for any reason, a system outage will occur. Lack of availability of the building may be caused by a true loss of the building through fire, explosion or the like. The building may also be unavailable for use as a TMC due to it being condemned for any number of reasons, or it may be inaccessible due to such occurrences as the loss of a road leading up to the building or a strike in front of the building.

Loss of infrastructure may be due to the failure of critical facilities needed within the building; typically power, communications, and/or water. Other infrastructure items may also require the evacuation of the TMC such as the loss of the fire detection system. Loss of any of these critical infrastructure items may result in a loss of the TMC infrastructure.

There are a number of mitigations for the infrastructure that may be considered to decrease the risk to the TMC. For the building, these include:

- u Carefully locate the TMC to not be in a flood plain or near the banks of a water body
- u Do not put a sign on or around the building indicating the functions
- u Build the TMC as a bunker

For power:

- u Locate the TMC in an area in which the building may be fed by multiple substations
- u Install and test a UPS and generator system
- u Insure that the UPS and generator will support all electric needs for the building

For communications:

- u Utilize multiple delivery mediums for communication technologies

Another approach to mitigation of risk for the infrastructure is the use of a redundant processing site. With the use of a redundant processing site, a second site exists that will mirror the primary TMC. The use of a redundant processing site provides the possibility of having no downtime in the event of the loss of infrastructure. With this type of processing site, the redundant TMC systems may automatically take over operations if/when the primary TMC becomes unavailable. This ability is predicated on an architecture where the hardware, software, and related data are mirrored between the primary and redundant sites. Mirroring the systems requires that any updates to the files are simultaneously written to both the primary and redundant disk drives.

In order to justify this type of approach, it is possible, and actually may be an advantage, to periodically use the redundant processing site. The site may be used during specific timeframes, such as during peak periods, during tests of the UPS and generator at the main processing site, or may be used by part of the staff for all normal processing. By using the redundant processing site the staff exercises its infrastructure, thus eliminating the need for additional testing.

When using a redundant processing site as a strategy within the mitigation plan, infrastructure issues must be reviewed in order to mitigate the impact of community-wide issues. When the redundant site is within the same area, the issues that caused a system outage at the primary site may also cause an outage at the redundant site. A rule of thumb that has been established by the financial industry regulators for distance between a prime and alternate site is 100 miles.⁶¹ This

distance is thought to be far enough to ensure that both sites will not be in the path of the same disaster.

The *Freeway Management and Operations Handbook*⁶² recommends that when an alternate site is used, TMC personnel should be prepared for being redeployed to the alternate site indefinitely, since alternate site may be used for a long period of time. If redundant processing is a chosen mitigation technique and the site is a significant distance from the prime site, living accommodations should be considered during a period of deployment.

With a redundant site, voice and data communications must be considered. Being able to continue communications at an alternate site may be accomplished in a number of ways. The communications lines may be rerouted to the alternate site as needed, which will provide continued communications capabilities. Alternatively, both the prime site and the alternate site may reside on the same network, thus allowing continued communications. In either case, the communications infrastructure should include multiple paths with each using a different technology to further reduce the risk. An example of multiple technologies is the use of telephone circuits and an alternate technology using internet connections through an internet service provider (ISP). When choosing an alternate communications path, it is important to ensure that the second path does not use the same equipment as the primary path, though they may seem like different products.

LOSS OF KEY PERSONNEL

People are key to the systems within the TMC. Without the staff being available the systems are incomplete. If not properly prepared, lacking key staff members can have the effect of causing system outages. Loss of key personnel may be caused by any number of reasons including:

- u Resignation
- u Retirement
- u Sickneses or epidemics
- u Extended vacation
- u Not available for any reason
- u Transfer to other jobs in other organizations
- u Job action
- u Reductions in force

Key personnel are defined as, in this context, staff members that are solely able to perform particular essential functions within the TMC. This may be a function of experience in performing a specific job or of specific knowledge that the staff member possesses.

There are several mitigations to the risk of the loss of key personnel. The most obvious mitigation is to avoid personnel turnover. Every manager is aware that avoiding turnover may be desired, but is not always possible. Given that turnover will happen, it is important to put processes in place that will mitigate the risk.

Periodically, management should review the existing staff and identify key staff members. Key staff members are those that, if they were not available to perform their duties, would cause significant problems in running the TMC. A succession plan should be developed to specify a staff

member that would be put into that position should the key staff member become unavailable. The backup that was identified may then be trained to a level that they could function in that capacity, if necessary.

An additional mitigation that should be undertaken is to document the functions and knowledge for all TMC staff members. In this way, any staff member is able to substitute for a staff member that is not present. The ultimate mitigation for loss of personnel is to conduct testing of the recovery plan using people who are not TMC staff. These people will test the plan using only the documentation supplied.

LOSS OF COMPUTER SYSTEMS

The computer systems are a vital part of the TMC systems. Loss of important computer systems will result in TMC system outages. Resources may be allocated in order to mitigate specific types of computer systems outages. As is true with other mitigations mentioned, these do not have the capacity to mitigate all computer system outages. The TMC environment should be reviewed to determine if any of these mitigations may be cost effective to institute.

As has been discussed previously in many other contexts, the specific definition of loss of computer systems is dependent upon the goals and mission of the TMC. When continuous availability is required, any loss of computer systems may impose a significant hardship. If all systems are required to be up and operational during morning and afternoon drive-times only, then there is more flexibility.

Loss of computer systems, in this context, may be caused by a hardware malfunction, a software error, or a combination of the two. Mitigation for other related causes are covered in other sections of this chapter.

The most expensive as well as the most effective mitigation is the use of a mirrored site which was already covered under the topic of “Loss of Infrastructure”. The same mitigation may be used also to mitigate many of the causes of computer system losses. When hardware errors occur, a mirrored site that may be used for fail-over will prevent computer system outages.

A basic mitigation technique is the requirement for virus protection to be run on all systems within the TMC. Even if the network is not open to the Internet, viruses may still be introduced into the system. Viruses are carried in emails, come from various Internet sites and even from media that is used on a system such as a CD. There have been some software packages that have been inadvertently sold with a virus embedded. In order to mitigate the issue of viruses affecting the computer systems, it is imperative that all computers run the latest version available of a credible virus protection program.

Instituting and enforcing policies that address access to the system are another basic mitigation for risk to the computer systems. Allowing only those people that need access and are trained in the system to have access is an important step in avoiding errors and malicious activities to affect the TMC’s computer systems. Basic access control includes removing access privileges from any employee who leaves the organization, either voluntarily or forced.

Software errors often are caused by the unexpected state of variables within the system. When the system is run from an alternate environment that is mirrored, it is possible that the variables will not be in the same state as those in primary environment. This difference may be caused by such occurrences as a minor electrical anomaly which causes one of a series of updates to inac-

curately post in the prime site. This same anomaly is unlikely to have happened in the same manner, at the same time in the mirrored site.

Testing and implementation of the system may be executed in a less risky manner using a mirrored site. Acceptance testing may be executed running against real-time data by using the mirror site hardware and network components. In this way the system may be easily exercised in the actual environment. If the system performs as expected it may then be put into service initially at the mirrored site. After a period of time that can act as a shakedown period, the system may then be moved to the primary TMC.

A full cycle of testing of any new software will mitigate risks. Testing of critical software should include full regression testing as mitigation for computer systems outages. Regression testing will perform tests on all functions that the system has always performed as well as functions that have been added to the system in the last changes.

Mitigation of hardware issues may be accomplished through the purchase of high availability hardware. High availability hardware will often contain redundant parts and the ability to switch automatically to them.

Failover software is an alternative to high availability hardware. This will monitor the health of the hardware/software system and, if necessary, automatically fail over to an alternate unit. In this way, if a hardware component becomes unusable, an alternate device will take its place.

Another mitigation to consider for hardware issues is preventative maintenance. Rather than waiting for a hardware failure, preventative maintenance will catch many hardware errors before they occur. Suggested scheduled maintenance therefore should be considered mitigation to hardware errors.

A final mitigation is the appropriate use of communications between staff members. A Change Control Board (CCB) is a committee, appropriately staffed, that reviews all changes to the TMC's systems before they are installed. An active CCB staffed with knowledgeable personnel from each of the areas within the TMC will anticipate problems before they occur. Each of the people representing the interest of their individual functions within the TMC should review the change in relationship to that function. In this way, unexpected effects of system changes may be considered.

COMMUNITY-WIDE DISASTERS

Hurricanes, floods, fires, riots, and terrorism are only some of the causes of disasters that may affect the community as a whole. Every time that we believe we have "heard it all" a new community-wide threat presents itself. The TMC is likely to have a role in providing for the well being of the citizens during these types of occurrences. With this as an organizational requirement, the TMC must find ways of mitigating the risk to the operations so that its services may still be rendered.

FEMA defines an emergency as any unplanned event that can cause deaths or significant injuries to employees, customers, or the public; or that can shut down businesses, disrupt operations, cause environmental damage or threaten a facility's financial standing.⁶³

From the TMC's perspective, a community-wide disaster is a little broader than the FEMA definition. A community-wide disaster may be planned. The result of Hurricane Katrina is considered a community-wide disaster and it was anticipated, albeit for a only days, beforehand. Fre-

quently storms, floods, riots and other can be anticipated with some level of knowledge of the future event that is expected.

In considering community-wide disasters the TMC should keep in mind that in research conducted by the Federal Transportation Administration it was determined that 58% of international terrorist attacks were on transportation targets, of these 92% were on surface transportation.⁶⁴ In a case of terrorism as indicated by these statistics, it is imperative that the TMC is available to assist in determining appropriate routes for responders to enter the area and routes for citizens to exit the area. The TMC may also have the function of helping keep the responders and the community aware of the state of the incident and actions that need to be taken. It is appropriate that the TMC be part of an Emergency Management Office during a community-wide emergency.

Many of the mitigations that have been discussed above will reduce potential risks that may occur during community-wide disasters. Each of the loss categories discussed above, infrastructure, key personnel, and systems, are not independent and may occur at the same time as any other loss.

Additional mitigations that may be considered for a community-wide disaster include additional security for the site, additional mitigations for devices that will be more important during these times and equipment that will aid in transportation and communications during emergency situations.

In the event of a community-wide disaster, the possibility of civil disobedience is ever present. No matter the nature of the disaster, panicked citizens will do whatever they feel that they have to in order to survive. This may include breaking into buildings and pillaging property. During periods of community-wide emergencies, mitigations for the TMC may include additional security staffing. By providing the TMC with additional security staff, the center will be maintained as a secure environment.

In a community-wide disaster there may be additional goals for the TMC. With the infrastructure of the TMC, and the training and knowledge of the TMC personnel, the TMC is likely to play an important part in recovery from the emergency situation. Information available through the roadway instrumentation that is available to the TMC is critical to the resolution of the emergency situation. In order to mitigate the risks that may occur during emergency situations an analysis should be completed that identify the particular devices. The devices and related communications infrastructure should be engineered for high availability. This may include alternate communications lines and alternate power supplies. Devices that may be considered are those that identify what is occurring in on the roadways and equipment used to advise the public of important information. Examples of this type of equipment include:

- u CCTV cameras
- u DMS
- u Road Weather Information Systems
- u Voice response systems
- u Internet sites

During periods of community-wide emergencies it is often complicated to transport personnel to the TMC. In order to mitigate the risk of having staff members unable to get to the TMC, alternate transportation methods may be put in place that can be deployed. Depending upon the type

of emergency situation that is most likely to occur, these may include vehicles such as boats or 4-wheel-drive cars.

MITIGATION OF RISK FOR PERIODS OF RECOVERY

Another look at the issue of mitigation of risk involves mitigating the risk of not being able to recover from a system outage. If a recovery is necessary it is vital that the TMC is able to recover within the timeframe that was specified in the goals of the organization.

The prime risk mitigation is the completion and ongoing testing of the recovery plan. This will cover all of the possible risk mitigations available. In the period of time that the TMC is having the project approved and up until the plan has been completed and the staff trained there are mitigations that may be put into place to move in the right direction. Specific tasks that will later become part of the ultimate solution may be started before the planning has been started. These functions will later become important portions of the plan. In fact, these tasks may be put together and documented to become a first version of the plan. Not a place to stop planning, but the place to begin planning for the TMC recovery.

Finding an appropriate alternate site is a fundamental starting place. The alternate site should be far enough away from the primary site that it is unlikely to be effected by the same problems that are affecting the primary site. The site should also be supplied by different telephone company central offices and power substations. See chapter 3 for a more complete discussion of selection of alternate sites.

Staffing of the alternate site is another basic mitigation that may be addressed during the pre-planning process. Forming a recovery team is an important start to this function. Personnel that represent each of the various functions within the TMC must be included. Others outside of the TMC organization may also be included such as representatives from the financial staff and the public relations staff may also be needed as a member of the team. See chapter 3 for a more complete discussion of staffing a recovery team.

Even with a recovery team in place, it is important to begin informing the staff as a whole of the expectations for them during relocation to an alternate site. Care should be given to the needs of staff members that will be displaced during these periods of recovery. The families must also be considered when planning for these staff members relocation to the alternate site. A more complete discussion of staffing issues is included in chapter 3.

One of the most basic mitigation that should be accomplished is backing up the system, storage of the backups and testing that restoring the system can be accomplished correctly. Each of these factors should be reviewed in context of the specific objectives trying to be met. System backups incur both hard and soft costs to the organization. The hard costs are related to the hardware and software needed to do the backups as well as any personnel costs and storage costs for the files. Soft costs usually are a greater issue to the organization than allocating the money for the hard costs. The soft costs are based on the time window that is necessary to do the backups. During this timeframe the system is usually required to be unavailable. As the system grows, the needed timeframe also grows. Finding an appropriate timeframe is often a challenge.

Daily backups should be accomplished only on data that is added or changed daily. Some examples of this type of data are operations logs, signal logs, incident logs, archives and CCTV images. The system (applications and operating system) itself does not change on a daily basis. Be-

cause of this, there is no need to back the system up on a daily basis. The system may be backed up when it is initially installed or changed, or may be backed up as part of a full system backup. Full system backups should be accomplished on a scheduled basis when there is a large window of time available to perform the backup. For this reason, many organizations do a full system backup on Sunday nights. Backups accomplished on a daily basis may either backup specific files that are known to change daily, or may do an incremental backup which backs up any files that have changed since the last backup was accomplished.

Full backups normally take far longer to run than partial or incremental backups. In restoring the data the opposite is true. If a full backup were accomplished every day, restoring the files would involve restoring the full backup only. When partial or incremental backups are being done, to accomplish a restoration the last full backup must be restored followed by each incremental backup in the order that they were created.

Storage procedures of the backups must also be reviewed carefully. The objective of the storage process includes

- u Backups being stored away from the TMC so that if access to the building is restricted the backups may still be available
- u Backups are stored in a manner that the media will remain intact
- u Backups are available for recovery 24 hours per day, 7 days per week
- u Backups are available quickly for recovery of a system failure where the TMC is available

The last bullet listed is the one that frequently confuses the issue. The latest backup is convenient to keep locally so that when an error occurs it can be corrected quickly. By keeping the current backup locally, the first bulleted requirement is no longer met. This may be solved by making two copies of each backup, keeping one onsite and sending the other offsite. Another possible solution is to have the current day's backup onsite, with the previous day's offsite along with the current day's log file that may be used to update the previous file with the log file.

Backing up the system and storing the backups appropriately become academic if the restore is not able to be executed successfully. See Chapter 6 for a discussion of this issue.

Mitigation will never eliminate the total risk of system outages. In fact, a decision may validly be made to not institute all possible risk mitigations. A risk analysis should be performed during each suggested mitigation to determine the probability of the risk, the related effects that the related outage would cause and the cost of the mitigation to determine if it is an appropriate investment for the TMC.

⁵⁹ "What is Business Continuity Planning?: How does it Differ from Disaster Recovery Planning?", *Disaster Recovery Journal*, Volume 15, Issue 1, Winter 2002

⁶⁰ *Integration of ITS with Security Systems in a Multi-Modal Environment*

⁶¹ Crosman, Penny Lunt, "A Watertight Plan", September 1, 2005,

<http://www.itarchitect.com/shared/printableArticle.jhtml?articleID=169400810>

⁶² *Freeway Management and Operations Handbook- Chapter 12: Freeway Management During Emergencies and Evacuations*

⁶³ *FREEWAY MANAGEMENT AND OPERATIONS HANDBOOK, FINAL REPORT, Federal Highway Administration, September 2003*

⁶⁴ *FREEWAY MANAGEMENT AND OPERATIONS HANDBOOK, FINAL REPORT, Federal Highway Administration, September 2003*

6

TESTING PREPAREDNESS

Chapter 6 Purpose:

To review methods that may be employed for testing recovery and mitigation for the TMC. As a part of testing, the need for a continuous improvement cycle is reviewed.

Chapter 6 Key Message:

- u Reasons for testing of TMC recovery and mitigation
- u Periodic testing is required
- u Need for continuous improvement of documentation

As has been discussed previously, testing is the most important part of the recovery and mitigation project. Performing adequate testing provides various benefits. Operational benefits are provided, while at the same time operations management is supplied with needed assurances that the plan will be successful during an actual event.

Testing is an ongoing process. In order to insure that the TMC's recovery and mitigation plan is always available and current, the plan must be continually tested. Periodic tests have the added benefit of reminding the staff of the necessity and requirements for recovery and mitigation. In that way they are more likely to keep this in mind during their daily work.

PURPOSE OF TESTING THE PLAN

Testing of the recovery and mitigation plan is vital to the TMC organization for various reasons. The testing process, at a minimum, will accomplish:

- u Validation and update of the recovery procedures and information contained within the plan (i.e. phone numbers, passwords)
- u Increasing personnel preparedness, both internal to the TMC and across organizational boundaries
- u Ensuring stakeholders understand the need for, and the extent of the preparedness for recovery of the TMC

The act of testing the recovery and mitigation plan validates that the plan works as expected and can be adapted to the constant changes associated with the systems in the TMC and the environment around the TMC. To ensure that the plan works as expected, it is vital to regularly test the plan according to a schedule that meets the needs of the TMC and can address system changes in a timely manner. In carrying out the testing, the team is revalidating that the plan continues to meet its goals. Validation of this type ensures that changes made within the TMC systems, non-systems processes in the TMC, and changes occurring outside the TMC are taken into account in

the plan. Such seemingly innocuous changes as the addition of telephone area codes in an adjoining state can require changes, albeit minor, to the plan. More serious issues may include such things as new protocols implemented regarding communications with other agencies, different systems within the TMC, and new policy issues that have not yet been addressed in the plan.

Correction to existing recovery and mitigation documentation is important because it keeps the plan current and usable. Currency of the plan allows it to be executed by individuals other than those with primary assignments. Notes should be kept during the testing in order to provide discussion material for potential corrections and/ or updates to the plan. All participants should take notes during the testing while additional information may be gathered by one or more observers.

As an outcome of the ongoing testing process, both the participants and the observers are likely to determine more efficient and effective ways of performing the tasks in the plan. Improvements may be a function of new processes and procedures being used in the TMC or improvements that are noticed during the execution of the testing itself. In either case, these improvements should be documented for future execution.

During the test review meeting, all suggested changes should be discussed. Assignments for preparation and insertion of the changes into the plan are then made. Any updates to the plan must be reviewed and accepted by personnel with the appropriate authority. Upon completion of updates to the plan, all physical and electronic versions must be updated or replaced by the new version. Version control procedures must be utilized and should include a version history of the plan being maintained in each copy, dating page updates, and numbering pages to allow for the insertion of pages.

It should be remembered that success in testing does not equate to every test being successful. Success in testing is often measured by the number of comments that are received that either corrects or improves the existing plan. A test that comes out with no comments and improvements is a test that has not exercised the plan enough and should be examined to try to make it more strenuous in the future.

The testing is also a vehicle that provides ongoing preparedness for the recovery team. Testing provides the team the ability to renew their skills and knowledge of the testing environment and plan. Expansion of the team through the participation of backup team members and new team members may be facilitated by the use of testing to introduce recovery concepts to prospective team members. There is no better method of exposing people to recovery and mitigation than through this type of participation.

Working together on a recovery test aids in camaraderie. The members are pulling together to accomplish an understood goal. Team members support each other during the testing in order for the test to be a success. With tests that are held with TMC staff, the result is likely to be internal staff members understanding each other better and able to work together more effectively on a daily basis. Tests may also be run within the wider organizational community.

Tests that are run which bring diverse agencies into the scenarios result in the additional advantage of bringing those from different agencies into a close working relationship striving for the same ultimate goal. During the preparation for the testing, the testing itself and the ultimate review of the test these team members gain a closer personal relationship. The outcome will be a closer working relationship between diverse agencies during other than testing and recovery operations. When communicating with these various agencies on a daily basis, team members will

able to “connect a name with a face”. They will be able to contact a person that they know through the testing, and a person that they will likely see again in the future at another recovery test.

Preparation for the testing goes a long way to reminding the staff of the importance of recovery and mitigation to the organization. It is another time that the staff has the opportunity to think through the need for and importance of this effort. As staff members prepare for the upcoming testing, any staff members not specifically included are likely to over-hear preparations. They are likely to be swept up by the “mob psychology” that revolving around a well organized testing preparation and aftermath. This is a prime time to encourage all staff members to keep preparedness in mind, embedding it into all operational processes and procedures.

Periodic testing gives stakeholders the assurance that operations are secure. It reminds them of the importance of recovery to the TMC operations while demonstrating the ability for the recovery to be accomplished. Both of these concepts are important for ongoing support of the operational program within the TMC.

TMC recovery and mitigation is an easy concept to be overlooked by stakeholders with the day-to-day issues that arise in every TMC operation. That is, until a recovery becomes necessary, where the stakeholders are able to have taken the correct path in support of the program. The testing process may be used to reinforce the need for this important function within the TMC. At the conclusion of the testing, all stakeholders should be supplied with a report on the test that has been conducted.

In reviewing the test report the stakeholder is familiar with the procedure that was undertaken, the successful exercising of the plan, the changes to be made and the required next steps and action items. When the report is correctly prepared it should also point out the level of preparedness that exists within the current TMC organization. Stakeholders may then increase the priority of recovery and mitigation within the organization, if warranted.

BEGINNING THE TEST PLANNING PROCESS

In order to meet the expectations of the testing, it is important to begin the process by defining a *test plan* that outlines each individual test that will be executed and include notes about which section(s) of the recovery and mitigation plan are covered by each test. As a part of this plan, a scenario should be defined for each test that will be attempted. Success criteria should be determined and documented for each test. Examples of matters to be addressed in this Test Plan include documentation, location, communications, infrastructure, participation, and the ability to restore normal operations.

Testing should exercise the recovery and mitigation documentation in order to verify that it is valid and usable. Expectation of documentation should be included and specifically reviewed as a part of all testing. Validation of the documentation is an outcome of each individual test. When a test fails, for any reason, the first item reviewed for the possibility of correction is the documentation. But, given that, an additional check on the validation of the documentation may be performed by having alternate personnel perform the testing.

As part of the test plan, specific directions should be provided for each test, in “cookbook” fashion. Having an alternate person perform the testing may ensure the tests are performed according to the written directions. The person most knowledgeable of the specific testing is likely to per-

form the test without specifically reading the instructions or performing the steps as they are written. This process has the added benefit of lowering the risk of the loss of specific personnel. Having others execute the test scenario, not being as familiar with the process, gives the ability to have others perform in that capacity.

As a sub-function of all testing, an evaluation of the ease of use of documentation should be assessed. This may be done as a discussion of the desire for this information before the test, and a debriefing of the information after the tests. It may be accomplished by having a comment section for these types of comments after each individual test case has been executed. Or, the ease of use of the documentation may be determined by an outside observer keeping notes on improvements during the time of the test.

Within the tests being executed, location of the specific recovery site should be considered. This should include expectations for recovery at a location other than the planned alternate, the ability to make needed changes at the alternative site, as well as being able to assess the system performance at the alternate site.

Periodic backups have been thought of as a rule-of-thumb minimum for recovery and mitigation. As discussed earlier in this document, a minimum testing requirement to test restoring the backups in order to determine that the backup files have been stored correctly. The proper method of performing this type of testing is for the restore to be accomplished at the actual backup location using the equipment that will be used in the case of a recovery. In performing this type of testing, assurances can be made as to the actual validity of the backup process and the compatibility of the equipment in the primary site with that in the alternate site.

The alternate site should be tested to ensure that it operates as expected. This includes both the performance that is expected from the site and the ability to modify the configuration at the alternate site. Testing may include the collection of metrics on the performance at the alternate site. This will require both the restoration of the alternate site and setting up workstations to monitor the response time.

The alternate site should be tested to ensure that there is the ability to configure needed changes. When the TMC must divert to an alternate site, it is likely that the diversion will continue for a considerable period of time. In a case of this type, it is important to be able to maintain the system, often making seemingly minor changes in order to facilitate operations from an alternate location.

Of those TMCs that have experienced significant outages, a number have considered communications to be the most significant matter that has been encountered. Communications should be included in the test plan in relation to:

- u Initial notification: the decision that a recovery situation has occurred
- u Intra-agency: mobilization of the team
- u Interpersonal and interdepartmental: operations during and following the recovery
- u Data communications: the alternate site functions as expected

During the review of the testing that has been accomplished, an examination may be held to review the participation of various agencies that must work together to affect a positive recovery. The review may include the agencies that would be useful to participate in the future, the level of participation from each agency and the method to handle the interagency communications.

Other infrastructure items should also be tested as part of the periodic test cycles. One item that should be primary to testing is backup electricity. Electricity backup, normally considered mitigation rather than a recovery device, should be tested in order to ensure that the equipment is working and that the capacity remains appropriate. As the TMC changes, even in little ways, the requirement for electric capacity is likely to change. Periodic testing of the electricity backup devices, including uninterrupted power supplies (UPS), and generators ensure that the TMC is able to operate appropriately without public electricity being available. The tests for electricity may be conducted at different times than the recovery testing. One TMC reports that they perform this type of testing weekly during the peak driving and electricity usage periods.

One often overlooked concept that should be included in the test planning is the ability to return to the original TMC site. As discussed earlier in this document, returning to the TMC is a process that is as complicated as originally leaving the TMC for an alternate site. The testing and review should cover both actions that have to be performed at the point that the move-back is being accomplished and procedures that have to be accomplished during the time running at the alternate TMC in order to facilitate the ultimate return.

TYPES OF TESTING

There are several types of testing that may be used to validate the recovery and mitigation strategy and plan. The primary types of testing may be referred to as “tabletop testing” and “full testing”. Each of these types of testing has their own positive and negative aspects. A combination of these test types may be used to minimize hard and soft costs while providing the maximum benefit to the TMC.

Tabletop testing, also known as classroom exercises or walk through testing, consists of the test team congregating in a room and talking through the handling of individual scenarios. The scenarios are cases which have been prepared before the testing sessions begin. The scenarios should be a complicated set of events that when taken together would cause an outage condition in the TMC. The scenarios should include an initial event or events that cause the response and secondary events that occur because of the initial event(s). An example may be (note: this scenario actually occurred)

- u Significant snowstorm
- u Airplane crashes into a highly traveled bridge
- u Plane passengers in the water
- u Cars hit on the bridge
- u Injuries and deaths in vehicles on the bridge
- u Subway accident with train jumping track, pinning person against wall
- u Traffic slowed to a stop in the area

By having appropriate team members in attendance thinking through the implications of the activities within their sphere of influence the team may find previously overlooked holes in the plan. Sophisticated scenarios, such as the one presented above, are virtually impossible to simulate as part of full testing. But, running through the thought processes of each of the recovery steps allows these overlooked areas to be addressed.

Full testing can exercise the complete process of restoration and running the TMC from an alternate facility. This type of testing begins with ensuring that the TMC can be reestablished at an alternate site, and once established, can operate from that site. Successful culmination of the initial testing proves many of the fundamental recovery and mitigation functions such as

- u Assurance that the backups are being accomplished correctly
- u Backup files are accessible during a recovery situation
- u System restores will run appropriately
- u Communications lines can be rerouted correctly
- u Documentation is accessible during a recovery situation
- u Passwords are correctly documented
- u The recovery team can be activated and assembled
- u Interpersonal intra-departmental communications work appropriately
- u Interpersonal inter-departmental communications work appropriately
- u Lines of authority are appropriate and understood
- u Education of the recovery team and/or alternate recovery team has been improved

Once the TMC has successfully exercised the basic full testing, additional constraints should be added to the full testing. Constraints will provide assurances that the TMC is prepared for an actual disaster and that decisions will not have to be made during a possible crisis situation. Examples of additional constraints that may be added to the base full test are

- u Non-preplanned test
- u Particular people are not present and alternates must execute from documentation
- u All communications cut and can not be restored
- u Test is planned, but no one knows what the issues will become
- u Test of assessing the damage and whether an alternate site is needed
- u Documentation is not available for a portion of the test or for the full test
- u Multiple agencies are executing a recovery concurrently

TIMING OF TESTS

It is critical to determine both the frequency and the timing of future tests as early as possible so that appropriate preparations and scheduling may be undertaken. Of most importance is to determine a reasonable frequency of testing. The frequency should be codified and management should respect the frequency that has been established. By maintaining a predefined frequency for testing, the staff can set expectations of upcoming work and management may more easily budget for testing in each upcoming year.

The frequency should take into account both tabletop and full testing. A useful tool in determining the appropriate frequency and type of testing is the test plan. In the plan, a strategy should be laid out that covers both the type and frequency of testing along with the objectives of each of

the tests. Each TMC will have different goals for their recovery and mitigation program and the related testing. Depending upon the specific goals it may be decided to use only full or full along with some tabletop testing. No matter the goals, it is imperative that some amount of full testing should be accomplished every year by the TMC. This will ensure that at least a fundamental recovery can be executed.

As a part of an annual TMC planning process, the dates corresponding to the approved frequency of testing should be determined. These should be determined far enough in advance so that the staff may be prepared and understand the testing objectives for each of the individual tests. It is also important that the appropriate people are available for each of the tests, whether tabletop or full tests.

REVIEW OF TESTING

A final portion of testing that is important in order to be able to provide continuous improvement to both the planning and the testing cycle is the review of each test. Each test should be staffed with an “auditor”. The auditor may be an internal auditor, or alternatively, a person that is educated in the testing process and documentation without any predetermined ideas about the test process results. The auditor should be known to all team members as a person that is there to record the results of each of the processes. They should record both what has occurred and ideas that they are given or that they come up with on how to improve the process and testing in the future.

As soon as possible after the testing has been completed the team should gather and evaluate the accomplishments of the testing. If possible the gathering should take place directly after the conclusion of the testing. In addition to reviewing the individual processes with their associated conclusions, an action item list should be generated. Each action item should be assigned and a completion date established. Action items should be followed up on periodically (i.e., each week) to ensure that they are completed in a reasonable amount of time. Errors that occurred during the testing should be specifically retested in the next test. If the same error occurs more than once, the status of the individual item should be reported to management. Minutes of the review should be distributed to all stakeholders.

7

ONGOING SUPPORT OF THE PLAN

Chapter 7 Purpose:

To point out the need and requirement for ongoing support of the recovery and mitigation plan. The plan and potential outcome during a system outage is only as good as the plan documentation is current. Information will be presented to encourage management to make an ongoing commitment to the need for and process of updating the plan.

Chapter 7 Key Message:

- u The recovery and mitigation documentation must be updated consistently in order to continue to be of value to the TMC.

A final issue that must be addressed is the ongoing support of the plan. A lot of work has gone into creating the recovery and mitigation plan as well as planning for and conducting the related testing. In order to create a continually improving plan, to keep the plan current and to correct errors that are found a process for ongoing support and upgrades for the plan must be instituted.

Risk priorities also vary over time. Old risks are replaced and overtaken by new risks. Many times the change in priority of various risks are a function of the latest disaster, either natural or man-made, to have adversely effected others. The risks that are of prime importance to the stakeholders of the TMC must be addressed in the recovery and mitigation plan.

In order to maintain credibility of the plan itself and the associated documentation, it is imperative that standard configuration management procedures are followed. Utilization of configuration management for the documentation allows for tracking changes that have been made along with the originator of and reason for the change.

Versioning is also used as part of configuration management in order to facilitate updating or replacing the copies of the plan that has been distributed. Any old copies of the plan should be returned to the responsible party to be accounted for and destroyed. Out-of-date copies of the plan both frustrate team members trying to accomplish a complex task and diminish the perception of credibility of the overall planning effort.

MANAGEMENT COMMITMENT

Management must make a commitment to ongoing support of the recovery and mitigation plan and related documentation. This includes support for both financial and organizational issues. Management support assures that the proper resources will be left in place so that the plan does not fall into disuse.

Ongoing financial support requires management to continually remind the budget officials of the need for and cost of recovery and mitigation. Depending upon the financial model that is used by

the individual TMC, such items as staffing, alternate sites, infrastructure costs, and test costs should be considered.

Budgeting for additional staff, possibly including a professional recovery and mitigation coordinator will ensure that the appropriate number of resources will be available. Consideration during the budgeting cycles should be given to the extra work that will be required of many of the staff members in reviewing and updating the documentation as well as participating in the testing cycle.

The use of any type alternate site is likely to have an associated recurring cost. On the high-end, the cost may be a subscription fee for using a commercial recovery site. Some other possible costs include maintaining equipment in the alternate site and rental allocations. The specific costs will be a function of the accounting process that the municipality employs.

Recovery and mitigation requires the expenditure of funds on infrastructure within the TMC. These costs may already be included in the standard operations budget, and if so, may be reclassified as an expense of this type. If not, these expenses should be considered for future budgeting. Examples of the additional infrastructure items needed are for the computer infrastructure, communications infrastructure, and the electric infrastructure.

The computer infrastructure has ongoing requirements for both recovery and mitigation. These include subscriptions to virus protection services, maintenance for upgrading all operating system and applications software, equipment and expendables for periodic backups of the system and off-site storage of the backups.

Ongoing communications costs include lines and equipment that are not used unless and until a recovery situation presents itself such as lines to be used for data communications with the alternate facility during a recovery situation. Other communications costs to take into account include devices and services supplied to staff members in order to more quickly make them available in the event of a recovery situation. Devices such as cell phones, beepers and cellular data services are examples of this type of communications equipment to be supplied to selective staff members. An additional communications cost, as mentioned previously in chapter 2, subscription access to Government Emergency Telecommunications System (GETS) and Wireless Priority Service (WPS) may be needed to allow priority voice communications during an emergency situation.

The electric infrastructure requires ongoing spending to maintain an uninterrupted power supply (UPS). A UPS needs to be periodically tested and maintained in order to keep it in working order. It should also regularly be reviewed to ensure that the unit will continue to support the equipment that is appropriate.

A final example of items that should be included in ongoing budgeting is the testing itself. Depending upon the accounting methods used by your TMC, testing can end up becoming a significant, ongoing cost. Included in the testing costs can be personnel time for the team preparing for the test, executing the test, and making changes after the test; transportation to an alternate site and use of alternate site.

COMMITMENT OF ONGOING SUPPORT OF PLAN

Many parts of the plan require to be reviewed periodically for possible update. IBM suggests that, among other items, the following should be reviewed periodically in order to keep the plan up to date and useful for the TMC.⁶⁵

- u Operational requirements – Investigate the changes in the TMC mission and procedures. Where required, the plan should be updated in order to match updated TMC direction.
- u Security requirements – Changes in security policies and procedures will require analogous changes to be made in the recovery and mitigation documentation. This can include such things as the process for adding personnel to the system, signing on, the process for entering the facility and personnel issues with employees leaving the TMC employment.
- u Technical procedures – New hardware or software changes may require changes in operational procedures. Changes of this type are likely to require equivalent changes in the recovery and mitigation plan. The changes to the recovery plan may be the same as those made in the TMC operations manual, or they may be changes that are required in reaction to the changes made in the primary TMC operations.
- u Hardware, software, and other equipment (types, specifications, and amount) – As described earlier, the recovery and mitigation documentation includes an inventory of all of the TMC assets. As the primary site updates and makes changes these must be reflected in the documentation. In making this type of change, it will allow the state of the primary TMC to be understood and reconstructed as necessary.
- u Names and contact information about team members – Team members will change on a periodic basis. Changes will occur due to staff leaving, new staff being hired, or current staff changing areas of responsibility. Additionally, staff contact information is likely to also require updates from time to time. Names (in case of marriage), home phone numbers, cell phone numbers, beeper numbers, home addresses, email addresses and the like will periodically change. Member information of the recovery team must be kept current in order to effectively contact personnel when needed.
- u Names and contact information about vendors, including alternate and off-site points-of-contact – Vendors for the TMC are important parts of the organization. Specific vendors change periodically as new contracts are let and assets are changed. Points-of-contact representing these organizations, as well as the method of contacting them and the related service level agreement allow working effectively with these organizations during redeployment to an alternate facility.
- u Alternate and off-site facility requirements – Just as the TMC makes changes to their environment, so does the alternative site. Any changes to the alternate site are likely to have an affect on the process that is required to restore operations of the TMC.

From a higher level, IBM also suggests that the Business Impact Analysis (BIA) should be periodically reviewed and updated to incorporate changes to contingency requirements and the related priorities. The BIA is meant to reveal vulnerabilities in the organization and develops strategies to minimize their risks. Policies, operational procedures, and risks within the organization must be reanalyzed in order to assure that the recovery and mitigation plans are consistent with what is being accomplished within the TMC.

In addition to periodic annual reviews of the plan, the *Disaster Recovery Journal* recommends that specific trigger events should cause a review of the recovery and mitigation plans. Examples of trigger events are:⁶⁶

- u Major hardware upgrades
- u Major software upgrades
- u Development projects
- u Significant personnel changes such as reorganizations, layoffs, promotions.
- u Policy changes
- u Procedural changes
- u Vendor changes

These updates may be handled as part of a periodic review of the recovery and mitigation plan which is recommended to be an annual update. Many of these individual items are likely to have significant changes in that period of time. Some of these changes may be made as a function of the changes occurring, such as the Human Resource system automatically updating the information as contact information is updated in their system.

PRIORITIZATION OF DOCUMENTATION

The Info Tech Research Group reminds us that once the initial task is complete, “whatever you do, please don’t feel that your task is complete. In fact, it is just beginning.”⁶⁷ Knowledge gained during the testing and updates precipitated by alterations in the environment must be added to recovery and mitigation documentation in order to keep the documentation in a usable form. These changes will add to the effectiveness of the documentation.

With the need to keep the plan updated, it is essential that TMC management place a priority on the continuation of maintenance of the recovery and mitigation plan. Tasks within a TMC are forever multiplying with many of them deemed as being as high priority. These tasks frequently have to be accomplished quickly. They are “drop everything and handle this”.

In times where there are more tasks to be accomplished than qualified personnel to handle them, it is hard to keep attention on the tasks related to a situation that (hopefully) will never occur. During situations of this type, management must remain vigilant keeping priority at the appropriate levels. This may be accomplished by assigning the responsibilities to a staff member with no other functions within the TMC. Another approach may be to have weekly status reporting on the progress of each task. The progress reports can be distributed to senior management within the TMC. Management then has the ongoing ability to “recommend” the relative priority of tasks that have been assigned as part of the recovery and mitigation project.

⁶⁵ Warrick, Cathy, et al, *IBM TotalStorage Business Continuity Solution Guide*, International Business Machines Corporation, 2005, ISBN 0738491136

⁶⁶ “What is Business Continuity Planning?: How does it Differ from Disaster Recovery Planning?”, *Disaster Recovery Journal*, Volume 15, Issue 1, Winter 2002

⁶⁷ Info Tech Research Group, *Building a Comprehensive Disaster Recovery Plan*, 2005 (ISBN 0-9730108-7-8)

8

SUMMARY

Chapter 8 Purpose:

To present a compendium of important points which have been presented within the paper.

Chapter 8 Key Message:

- u Preparing for recovery and mitigation is important to the TMC
- u Policy decisions to support recovery and mitigation
- u Management direction that support the recovery and mitigation effort

Within the seven chapters above, information and explanations have been presented covering many of the issues involved in avoiding and preparing for a system outage within the TMC. Many of the ideas and concepts that have been covered previously are listed within this chapter as checklists to be considered at various points within your project. Each individual item includes a reference to the area of the preceding document that more fully describes the action.

In the context of this chapter, it is important to remember, as presented in Chapter 1, that “*Operational systems are made up of hardware, software, people, facilities and procedures.*” Although significant effort is directed towards automated systems, the complete operational system within the TMC must be considered when developing the plan for recovery and mitigation.

PROJECT INITIATION

Each TMC and their respective management will have their own reasons behind beginning a recovery and mitigation project. These may be due to an organizational directive, news reports of recent disasters (hopefully) somewhere other than within your municipality or information received about the need for this type of effort.

No matter the reason for initiating the project, the following actions should be considered as a starting point for a recovery and mitigation project within the TMC.

Project Initiation

In Place	N/A	Action	Reference
<input type="checkbox"/>	<input type="checkbox"/>	Identify project sponsor	Ch. 2, “Policy Issues”
<input type="checkbox"/>	<input type="checkbox"/>	Publish TMC Mission Statement	Ch. 2, “Planning”
<input type="checkbox"/>	<input type="checkbox"/>	Obtain funding for, and prepare a Business Impact Analysis	Ch. 2, “Synthesis of Results & Best Practices”

The TMC Mission Statement allows all personnel to have a consistent goal when working on the Business Impact Analysis (BIA). The BIA will convert the TMC Mission Statement into operational terms. Once approved, the BIA may be used to determine budgets and act as the requirements for the remainder of the project.

The following checklist outlines actions to be taken into account in the BIA.

Business Impact Analysis

In Place	N/A	Action	Reference
<input type="checkbox"/>	<input type="checkbox"/>	Identify functions critical to TMC's operations	Ch. 3, "Business Impact Analysis"
<input type="checkbox"/>	<input type="checkbox"/>	Identify risks to the above functions	Ch. 3, "Business Impact Analysis"
<input type="checkbox"/>	<input type="checkbox"/>	Establish service level metrics for the TMC	Ch. 3, "Business Impact Analysis"
<input type="checkbox"/>	<input type="checkbox"/>	Rate (prioritize) risks by probability of occurrence and impact on the TMC	Ch. 3, "Business Impact Analysis"
<input type="checkbox"/>	<input type="checkbox"/>	Identify ways to avoid or mitigate identified risks	Ch. 3, "Business Impact Analysis"
<input type="checkbox"/>	<input type="checkbox"/>	Prioritize recommended avoidance and mitigation options	Ch. 3, "Business Impact Analysis"

PROJECT FUNDING

Once the tasks of publishing the TMC Mission Statement and developing the Business Impact Analysis are completed, you are ready to obtain funding for the remainder of the project. The following checklists outline remaining parts of the project that must be funded.

Project Funding

In Place	N/A	Action	Reference
<input type="checkbox"/>	<input type="checkbox"/>	Develop a budget and obtain approval to implement plan	Ch. 2, "Management Commitment"
<input type="checkbox"/>	<input type="checkbox"/>	Develop a budget and obtain approval to test the plan	Ch. 2, "Management Commitment"
<input type="checkbox"/>	<input type="checkbox"/>	Develop a budget and obtain approval for on-going testing	Ch. 2, "Management Commitment"
<input type="checkbox"/>	<input type="checkbox"/>	Develop a budget and obtain approval for on-going updates to the plan	Ch. 3, "Budget to Maintain Plan"

RECOVERY AND MITIGATION PLANNING

In order to move forward with recovery and mitigation, there are administrative processes that should be put into place. These administrative processes will allow the project to progress in a

defined manner. Approval of these documents will allow the team to circumvent policy difficulties as the project proceeds.

Recovery and Mitigation Planning

In Place	N/A	Action	Reference
<input type="checkbox"/>	<input type="checkbox"/>	Develop a change control plan for the project	Ch. 3, "Ongoing Support of the Plan"
<input type="checkbox"/>	<input type="checkbox"/>	Develop a version control process for documentation	Ch. 7, "Ongoing Support for the Plan"
<input type="checkbox"/>	<input type="checkbox"/>	Install a change control board for the project	Ch. 3 "Ongoing support of the Plan"
<input type="checkbox"/>	<input type="checkbox"/>	Develop an internal communication plan to be used during an outage	Ch. 4, "Internal Communications Policies"
<input type="checkbox"/>	<input type="checkbox"/>	Develop an external communication plan to be used during an outage	Ch. 4, "External Communications Policies"
<input type="checkbox"/>	<input type="checkbox"/>	Develop a document distribution plan for project documentation	Ch. 1, "Documentation"
<input type="checkbox"/>	<input type="checkbox"/>	Develop a management succession plan for period of system outage	Ch. 3, "Management Succession Plan"
<input type="checkbox"/>	<input type="checkbox"/>	Develop an occupant emergency plan for building evacuation	Ch. 2, "Documentation"
<input type="checkbox"/>	<input type="checkbox"/>	Develop a succession plan for key recovery team personnel	Ch. 3, "Continuity of Operations"
<input type="checkbox"/>	<input type="checkbox"/>	Document personnel roles and responsibilities for those involved in a recovery	Ch. 2, "Policies"
<input type="checkbox"/>	<input type="checkbox"/>	Define types of outages	Ch. 2, "Policies"
<input type="checkbox"/>	<input type="checkbox"/>	Develop responses to defined outages	Ch. 2, "Policies"

RECOVERY TEAM

The Recovery Team is activated and functions during the planning, testing, and an actual recovery situation. There are many functions to be handled during a recovery situation, which may be managed by separate teams or may be among the responsibilities of a single recovery team. Designations of suggested teams or functions are listed in the following checklist.

Recovery Teams

In Place	N/A	Action	Reference
<input type="checkbox"/>	<input type="checkbox"/>	Appoint a management team	Ch. 3, "Establish sub-teams"
<input type="checkbox"/>	<input type="checkbox"/>	Appoint a business recovery team	Ch. 3, "Establish sub-teams"
<input type="checkbox"/>	<input type="checkbox"/>	Appoint a departmental recovery team	Ch. 3, "Establish sub-teams"

In Place	N/A	Action	Reference
<input type="checkbox"/>	<input type="checkbox"/>	Appoint a computer recovery team	Ch. 3, "Establish sub-teams"
<input type="checkbox"/>	<input type="checkbox"/>	Appoint a damage assessment team	Ch. 3, "Establish sub-teams"
<input type="checkbox"/>	<input type="checkbox"/>	Appoint a security team	Ch. 3, "Establish sub-teams"
<input type="checkbox"/>	<input type="checkbox"/>	Appoint a facilities support team	Ch. 3, "Establish sub-teams"
<input type="checkbox"/>	<input type="checkbox"/>	Appoint an administrative support team	Ch. 3, "Establish sub-teams"
<input type="checkbox"/>	<input type="checkbox"/>	Appoint a logistics support team	Ch. 3, "Establish sub-teams"
<input type="checkbox"/>	<input type="checkbox"/>	Appoint a user support team	Ch. 3, "Establish sub-teams"
<input type="checkbox"/>	<input type="checkbox"/>	Appoint a computer backup team	Ch. 3, "Establish sub-teams"
<input type="checkbox"/>	<input type="checkbox"/>	Appoint an offsite storage team	Ch. 3, "Establish sub-teams"
<input type="checkbox"/>	<input type="checkbox"/>	Appoint a software team	Ch. 3, "Establish sub-teams"
<input type="checkbox"/>	<input type="checkbox"/>	Appoint a communications team	Ch. 3, "Establish sub-teams"
<input type="checkbox"/>	<input type="checkbox"/>	Appoint an applications team	Ch. 3, "Establish sub-teams"
<input type="checkbox"/>	<input type="checkbox"/>	Appoint a human relations team	Ch. 3, "Establish sub-teams"
<input type="checkbox"/>	<input type="checkbox"/>	Appoint a marketing/customer relations team	Ch. 3, "Establish sub-teams"

MITIGATION

The best outage is one that is mitigated. Based on the Business Impact Analysis that has already been completed, the following mitigations are examples of those that the TMC may consider. The following checklists discuss types of mitigations that the TMC may consider in order to lessen the risk of outage.

Infrastructure Mitigation

In Place	N/A	Action	Reference
<input type="checkbox"/>	<input type="checkbox"/>	Install a backup power generator	Ch. 3, "Infrastructure Mitigation"
<input type="checkbox"/>	<input type="checkbox"/>	Install a fire suppression system	Ch. 3, "Infrastructure Mitigation"
<input type="checkbox"/>	<input type="checkbox"/>	Install fire and smoke sensors	Ch. 3, "Infrastructure Mitigation"
<input type="checkbox"/>	<input type="checkbox"/>	Install water sensors	Ch. 3, "Infrastructure Mitigation"
<input type="checkbox"/>	<input type="checkbox"/>	Install an emergency master system shutdown switch	Ch. 3, "Infrastructure Mitigation"
<input type="checkbox"/>	<input type="checkbox"/>	Have plastic tarps for computer equipment available for use as needed	Ch. 3, "Infrastructure Mitigation"

In Place	N/A	Action	Reference
<input type="checkbox"/>	<input type="checkbox"/>	Install and use heat/water resistant containers for electronic media and other records	Ch. 3, "Infrastructure Mitigation"
<input type="checkbox"/>	<input type="checkbox"/>	Install and monitor video surveillance	Ch. 3, "Physical Security"
<input type="checkbox"/>	<input type="checkbox"/>	Install and use access control devices	Ch. 3, "Physical Security"
<input type="checkbox"/>	<input type="checkbox"/>	Ensure that critical equipment is properly placed	Ch. 3, "Physical Security"
<input type="checkbox"/>	<input type="checkbox"/>	Institute and enforce a policy prohibiting smoking & food/drink near equipment	Ch. 3, "Physical Security"
<input type="checkbox"/>	<input type="checkbox"/>	Develop a fuel tank refilling process	Ch. 2, "Planning"

Network Mitigation

In Place	N/A	Action	Reference
<input type="checkbox"/>	<input type="checkbox"/>	Install an uninterrupted power supply (UPS) for servers	Ch. 2, "Planning"
<input type="checkbox"/>	<input type="checkbox"/>	Install UPSs for workstations	Ch. 2, "Planning"
<input type="checkbox"/>	<input type="checkbox"/>	Install UPSs for router/switches/firewalls	Ch. 2, "Planning"
<input type="checkbox"/>	<input type="checkbox"/>	Install anti-virus software on servers and keep updated	Ch. 3, "Logical Security"
<input type="checkbox"/>	<input type="checkbox"/>	Install anti-virus software on workstations and keep updated	Ch. 3, "Logical Security"
<input type="checkbox"/>	<input type="checkbox"/>	Install anti-spyware software on servers and keep updated	Ch. 3, "Logical Security"
<input type="checkbox"/>	<input type="checkbox"/>	Install anti-spyware software on workstations and keep updated	Ch. 3, "Logical Security"
<input type="checkbox"/>	<input type="checkbox"/>	Architect, purchase, and install failover hardware	Ch. 5, "Loss of Computer System"
<input type="checkbox"/>	<input type="checkbox"/>	Architect, purchase, and install cyber-intrusion prevention i.e. firewall, intrusion detection)	Ch. 1, "Types of Mitigation"
<input type="checkbox"/>	<input type="checkbox"/>	Perform periodic data backups	Ch. 2, "Policies"
<input type="checkbox"/>	<input type="checkbox"/>	Maintain hardware by schedule	Ch. 5 "Loss of Computer System"

Telecommunications Mitigation

In Place	N/A	Action	Reference
<input type="checkbox"/>	<input type="checkbox"/>	Architect and install multiple data communication paths to the TMC	Ch. 2, "Planning"
<input type="checkbox"/>	<input type="checkbox"/>	Register for Wireless Priority Service (WPS)	Ch. 3, "Planning Generically..."

In Place	N/A	Action	Reference
<input type="checkbox"/>	<input type="checkbox"/>	Register for Government Emergency Telecommunications Service (GETS)	Ch. 3, "Planning Generically..."
<input type="checkbox"/>	<input type="checkbox"/>	Maintain "plain old telephone system" (POTS)	Ch. 2, "Low Tech Solutions"
<input type="checkbox"/>	<input type="checkbox"/>	Maintain dial-up modems	Ch. 2, "Low Tech Solutions"

Mitigation Policies

In Place	N/A	Action	Reference
<input type="checkbox"/>	<input type="checkbox"/>	Develop and enforce security standards	Ch. 2, "State-of-the-Art"
<input type="checkbox"/>	<input type="checkbox"/>	Develop and enforce hardware standards	Ch. 2, "State-of-the-Art"
<input type="checkbox"/>	<input type="checkbox"/>	Develop and enforce software standards	Ch. 2, "State-of-the-Art"
<input type="checkbox"/>	<input type="checkbox"/>	Develop and enforce operating system standards	Ch. 2, "State-of-the-Art"
<input type="checkbox"/>	<input type="checkbox"/>	Develop and enforce physical controls of TMC	Ch. 2, "State-of-the-Practice"
<input type="checkbox"/>	<input type="checkbox"/>	Develop and enforce logical controls of TMC systems	Ch. 2, "State-of-the-Practice"
<input type="checkbox"/>	<input type="checkbox"/>	Develop a policy for communications with the media and public	Ch. 2, "Synthesis of Results & Best Practices"
<input type="checkbox"/>	<input type="checkbox"/>	Develop and implement data backup methods and schedule (full and incremental)	Ch. 3, "Risk Mitigation"
<input type="checkbox"/>	<input type="checkbox"/>	Develop and implement data backup media and documentation retention schedule (approved by legal counsel)	Ch. 3, "Risk Mitigation"

Testing Mitigation

In Place	N/A	Action	Reference
<input type="checkbox"/>	<input type="checkbox"/>	Test generator tank refilling with generator running	Ch. 2, "State of the Practice"
<input type="checkbox"/>	<input type="checkbox"/>	Test backup power	Ch. 2, "State of the Practice"
<input type="checkbox"/>	<input type="checkbox"/>	Test alternate data communications paths	Ch. 2, "State of the Practice"

RECOVERY

When mitigations do not work the TMC may be faced with the need to recover its functionality at an alternate site. In order to successfully perform a recovery of this type, a plan must be developed, documented and tested. The following checklists contain examples of the actions to be taken in order to assure a successful recovery situation.

Documentation

In Place	N/A	Action	Reference
----------	-----	--------	-----------

In Place	N/A	Action	Reference
<input type="checkbox"/>	<input type="checkbox"/>	Document TMC standard operating procedures	Ch. 2, "State of the Art"
<input type="checkbox"/>	<input type="checkbox"/>	Document TMC policies and processes	Ch. 2, "State of the Art"
<input type="checkbox"/>	<input type="checkbox"/>	Document the network map	Ch. 2, "State of the Art"
<input type="checkbox"/>	<input type="checkbox"/>	Document all system passwords	Ch. 2, "State of the Art"
<input type="checkbox"/>	<input type="checkbox"/>	Document personnel contact list	Ch. 2, "State of the Art"
<input type="checkbox"/>	<input type="checkbox"/>	Document vendor contact list	Ch. 2, "State of the Art"
<input type="checkbox"/>	<input type="checkbox"/>	Document agency contact list	Ch. 2, "State of the Art"
<input type="checkbox"/>	<input type="checkbox"/>	Develop schedule for updating process, procedure, and contact list documentation	Ch. 2, "State of the Art"
<input type="checkbox"/>	<input type="checkbox"/>	Determine confidentiality of documentation by section	Ch. 2, "State of the Art"
<input type="checkbox"/>	<input type="checkbox"/>	Ensure that hard copies of plan are kept offsite	Ch. 2, "State of the Art"
<input type="checkbox"/>	<input type="checkbox"/>	Negotiate service level agreements (SLA) requirements with vendors	Ch. 2, "State of the Art"

Recovery Policies

In Place	N/A	Action	Reference
<input type="checkbox"/>	<input type="checkbox"/>	Develop a policy to loosen restrictions on procurement authority during an outage	Ch. 2, "State-of-the-Practice"
<input type="checkbox"/>	<input type="checkbox"/>	Develop a policy on personnel activation during an outage	Ch. 2, "State-of-the-Practice"
<input type="checkbox"/>	<input type="checkbox"/>	Develop a policy on who can declare an emergency	Ch. 2, "State-of-the-Practice"

Alternate Site

In Place	N/A	Action	Reference
<input type="checkbox"/>	<input type="checkbox"/>	Identify alternate site, select and contract	Ch 2, "Alternate Site"
<input type="checkbox"/>	<input type="checkbox"/>	Architect and contract for communication lines to be available at alternate site	Ch. 2, "Alternate Site"
<input type="checkbox"/>	<input type="checkbox"/>	Ensure that a full set of recovery manuals are available at alternate site	Ch. 3, "Planning Generically..."
<input type="checkbox"/>	<input type="checkbox"/>	Plan and establish physical security at alternate site	Ch. 3, "Planning Generically..."
<input type="checkbox"/>	<input type="checkbox"/>	Plan and establish logical security at alternate site	Ch. 3, "Planning Generically..."
<input type="checkbox"/>	<input type="checkbox"/>	Ensure that data backups are available at alternate site	Ch. 2, "Alternate Site"

In Place	N/A	Action	Reference
<input type="checkbox"/>	<input type="checkbox"/>	Ensure that software licenses are valid at alternate site	Ch. 3, "Planning Generically..."
<input type="checkbox"/>	<input type="checkbox"/>	Identify living accommodations for staff near alternate site	Ch. 3, "Planning Generically..."

Recovery Supplies

In Place	N/A	Action	Reference
<input type="checkbox"/>	<input type="checkbox"/>	Purchase and stock batteries for alternate site	Ch. 2, "Synthesis of Results & Best Practices"
<input type="checkbox"/>	<input type="checkbox"/>	Purchase and stock bottled water for alternate site	Ch. 2, "Synthesis of Results & Best Practices"
<input type="checkbox"/>	<input type="checkbox"/>	Purchase and stock first aid kit for alternate site	Ch. 2, "Synthesis of Results & Best Practices"
<input type="checkbox"/>	<input type="checkbox"/>	Purchase and stock flashlights for alternate site	Ch. 2, "Synthesis of Results & Best Practices"
<input type="checkbox"/>	<input type="checkbox"/>	Purchase and stock food for alternate site	Ch. 2, "Synthesis of Results & Best Practices"
<input type="checkbox"/>	<input type="checkbox"/>	Purchase and stock AM/FM radios for alternate site	Ch. 2, "Synthesis of Results & Best Practices"
<input type="checkbox"/>	<input type="checkbox"/>	Purchase and stock cellular phones for alternate site	Ch. 2, "Synthesis of Results & Best Practices"
<input type="checkbox"/>	<input type="checkbox"/>	Purchase and stock satellite phones for alternate site	Ch. 2, "Synthesis of Results & Best Practices"

Recovery Processes

In Place	N/A	Action	Reference
<input type="checkbox"/>	<input type="checkbox"/>	Develop process to activate alternate site	Ch. 4, "Establish the Following Policies"
<input type="checkbox"/>	<input type="checkbox"/>	Develop process to activate communication lines	Ch. 4, "Policy Issues"
<input type="checkbox"/>	<input type="checkbox"/>	Develop process to activate GETS and WPS	Ch. 7, "Management Commitment"
<input type="checkbox"/>	<input type="checkbox"/>	Develop process to distribute communication devices (i.e. cell phones, pagers etc.)	Ch. 3, "Planning Generically..."
<input type="checkbox"/>	<input type="checkbox"/>	Develop process to install additional security staff at alternate site	Ch. 5, "Community Wide Disaster"
<input type="checkbox"/>	<input type="checkbox"/>	Develop process to retrieve offsite stored data backup	Ch. 5, "Data Backup Storage"

In Place	N/A	Action	Reference
<input type="checkbox"/>	<input type="checkbox"/>	Develop process for documentation retention	Ch. 2, "Policies"

Recovery Testing

In Place	N/A	Action	Reference
<input type="checkbox"/>	<input type="checkbox"/>	Develop recovery testing schedule	Ch. 6, "Beginning the Test Planning Process"
<input type="checkbox"/>	<input type="checkbox"/>	Develop tabletop test plan and schedule	Ch. 6, "Types of Testing"
<input type="checkbox"/>	<input type="checkbox"/>	Develop full test plan and schedule	Ch. 6, "Types of Testing"
<input type="checkbox"/>	<input type="checkbox"/>	Develop a process for third-party testing observer	Ch. 6, "Review of Testing"
<input type="checkbox"/>	<input type="checkbox"/>	Develop and schedule a test of returning to TMC	Ch. 6, "Timing of Testing"
<input type="checkbox"/>	<input type="checkbox"/>	Perform post-test review	Ch. 6, "Review of Testing"
<input type="checkbox"/>	<input type="checkbox"/>	Plan and monitor updates after testing	Ch. 6, "Review of Testing"

Support for Personnel During a Recovery

In Place	N/A	Action	Reference
<input type="checkbox"/>	<input type="checkbox"/>	Develop procedure to move families of recovery team	Ch. 2, "Synthesis of Results & Best Practices"
<input type="checkbox"/>	<input type="checkbox"/>	Provide for child care for family of recovery team	Ch. 2, "Synthesis of Results & Best Practices"
<input type="checkbox"/>	<input type="checkbox"/>	Develop list of nearby restaurants for use during recovery	Ch. 2, "Synthesis of Results & Best Practices"
<input type="checkbox"/>	<input type="checkbox"/>	Develop list of nearby religious organizations for use during recovery	Ch. 2, "Synthesis of Results & Best Practices"
<input type="checkbox"/>	<input type="checkbox"/>	Develop list of nearby gyms for use during recovery	Ch. 2, "Synthesis of Results & Best Practices"

Field Devices

In Place	N/A	Action	Reference
<input type="checkbox"/>	<input type="checkbox"/>	Define and contract for alternate communication paths for field devices	Ch. 2, "State-of-the-Practice"
<input type="checkbox"/>	<input type="checkbox"/>	Define and install alternate power sources for field devices	Ch. 2, "State-of-the-Practice"
<input type="checkbox"/>	<input type="checkbox"/>	Secure portable devices for use during outage situations	Ch. 2, "Synthesis of Results & Best Practices"

In Place	N/A	Action	Reference
<input type="checkbox"/>	<input type="checkbox"/>	Secure portable generators for use during outage situations	Ch. 2, "Synthesis of Results & Best Practices"

RETURN TO THE TMC

After an outage requiring operations to be moved to an alternate TMC, care must be taken in moving back to the original or new-permanent TMC. The steps are much the same as was needed to move to the alternate site. The following checklist lists functions that are needed in order to move back to the TMC.

Return to TMC

Complete	N/A	Action	Reference
<input type="checkbox"/>	<input type="checkbox"/>	Ensure adequate infrastructure support, such as electric power, water, telecommunications, security, environmental controls, office equipment, and supplies	Ch. 4, "Planning to Return to TMC"
<input type="checkbox"/>	<input type="checkbox"/>	Install system hardware, software, and firmware. This activity should include detailed restoration procedures similar to those followed in the Recovery Phase	Ch. 4, "Planning to Return to TMC"
<input type="checkbox"/>	<input type="checkbox"/>	Establish connectivity and interfaces with network components and external systems	Ch. 4, "Planning to Return to TMC"
<input type="checkbox"/>	<input type="checkbox"/>	Test system operations to ensure full functionality exists	Ch. 4, "Planning to Return to TMC"
<input type="checkbox"/>	<input type="checkbox"/>	Back up operational data on the contingency/alternate system and uploading to restored system	Ch. 4, "Planning to Return to TMC"
<input type="checkbox"/>	<input type="checkbox"/>	Shut down the contingency/alternate system and terminating operations at that site	Ch. 4, "Planning to Return to TMC"
<input type="checkbox"/>	<input type="checkbox"/>	Secure, remove, and/or relocate all sensitive materials at the contingency site	Ch. 4, "Planning to Return to TMC"
<input type="checkbox"/>	<input type="checkbox"/>	Arrange for recovery personnel to return to the original facility	Ch. 4, "Planning to Return to TMC"

PLAN REVIEW

Recovery and mitigation plans should be reviewed both on a periodic (i.e. annual) basis and due to specific trigger events. The following checklist lists examples of trigger events that will require a plan review.

Trigger Events to Review Plan

Occurred	N/A	Action	Reference
----------	-----	--------	-----------

Oc- curred	N/A	Action	Reference
<input type="checkbox"/>	<input type="checkbox"/>	Major hardware upgrades	Ch. 7, "Trigger Events for Plan Review"
<input type="checkbox"/>	<input type="checkbox"/>	Major software upgrades	Ch. 7, "Trigger Events for Plan Review"
<input type="checkbox"/>	<input type="checkbox"/>	Development projects	Ch. 7, "Trigger Events for Plan Review"
<input type="checkbox"/>	<input type="checkbox"/>	Significant personnel change	Ch. 7, "Trigger Events for Plan Review"
<input type="checkbox"/>	<input type="checkbox"/>	Policy changes	Ch. 7, "Trigger Events for Plan Review"
<input type="checkbox"/>	<input type="checkbox"/>	Procedure changes	Ch. 7, "Trigger Events for Plan Review"
<input type="checkbox"/>	<input type="checkbox"/>	Vendor changes	Ch. 7, "Trigger Events for Plan Review"

This document is a starting point. It is a starting point to allow TMC management the ability to size and approach the effort of recovery and mitigation.

Over the years recovery and mitigation has been shown to be important to the community time and time again. No matter the cause of the system outage, the community is hurt if the operations system is not able to continue operations. Continuation of operations is known by different names such as COOP, Disaster Recovery Planning, and in this case Recovery and Mitigation. No matter what it is called, continuation of operational function is important to the health and welfare of the communities that we serve.