

# *NYSFIRM*

## *Government Information*

### *Focus*

#### *Supporting the Public's Business: Continuity Planning & NYS Government*

Linda Fisher Neidl

With support from:  
The NYS Forum for IRM  
IT Corporate Roundtable

## **Executive Summary**

In the aftermath of 9/11 (September 11, 2001) public and private organizations scrambled to reassess their plans for business continuance in the face of previously unimaginable parameters of disaster. This paper briefly reviews the history of disaster preparedness in New York State from the legislative study of this phenomenon in 1978 to the current creation of organizations and positions to better position New York to deal with the realities of post-9/11.

With the renewed and broadened thinking about dealing with disaster it is apparent that the concept of "business continuity planning" is a term that encompasses many of those terms and phrases previously used such as contingency planning, disaster preparedness, disaster prevention, and disaster recovery. This paper addresses the relationship of the historical approach to what is now encompassed by business continuity planning, and identifies the need for cohesiveness between business functions and supporting technology between development and implementation of planning decisions, and between and among agencies as vital to understanding and valuing this new and broader approach.

New York State Forum  
for Information Resource Management  
Rockefeller Institute of Government  
411 State Street  
Albany, NY 12203  
Phone (518) 443-5001  
Fax (518) 443-5006  
E-mail [info@nysfirm.org](mailto:info@nysfirm.org)  
Web [www.nysfirm.org](http://www.nysfirm.org)

Facilities, information, and personnel, the three facets of continuity planning, are described in this paper, delineating the scope, detail, and key considerations relevant to each that are critical to effective planning. The essential steps of impact and risk analysis and plan development and implementation are described and references are made to valuable planning resources and exemplars contained in the Appendices.

A number of essential resources are in place to assist New York's state and local government organizations with the process of business continuity planning. Moreover, a number of key entities and positions have recently been created to add the essential elements of support and coordination that are needed by those at the state and local government levels seeking assistance with planning. With these resources in place it is still important that: (1) the concept of continuity planning is elevated to a greater priority and routinely integrated into workplace procedures and budgeting; (2) responsibilities and leadership for continuity planning are clearly delineated; and (3) adequate resources are made available to state and local government organizations to affect ongoing continuity planning and testing cycles.

# *Supporting the Public's Business: Continuity Planning & NYS Government*

*New York State Forum for Information Resource Management White paper  
October 2002*

Linda Fisher Neidl

## **Contents**

*About the Author.....i  
Acknowledgements.....i*

*Introduction.....1*

*A Rationale for Readiness.....2*

*The Public's Business and Continuity Planning: What's in a Name?.....3  
    The Relationship to Disaster Planning.....4  
    Naming.....5*

*Whose Job Is It?.....7*

*State Emergency Management Office.....8*

*Office for Technology.....9*

*Office of Public Security.....12*

*Chief Information Officer.....13*

*What's Involved?...14*

*How It Works.....15*

*Initiation.....17*

*The Business Impact and Risk Analyses.....18*

*Plan Development and Implementation.....19*

*The Team.....20*

*About "How To" Resources.....20*

*Conclusion.....21*

*APPENDIX A: Glossary...23*

*APPENDIX B: On-line Resources....24*

*APPENDIX C: Sources Cited....26*

*APPENDIX C: Background Sources Not Cited....27*

## *About the Author*

Linda Neidl is a student of graduate studies in the MSIS Program with an emphasis in policy analysis at the University at Albany. Through a collaborative arrangement with the University at Albany, Ms. Neidl served an internship at The Forum with the explicit assignment of preparing this business continuity white paper as a research and analysis endeavor. We are grateful to Linda for her research, conclusions, and recommendations. The recommendations are clearly appropriate and will serve to shape future Forum initiatives related to the furtherance of state and local government capacity to adequately plan and implement business continuity measures.

## *Acknowledgements*

The Forum wishes to extend its appreciation to Robert Freeman, Executive Director of the Department of State Committee on Open Government, JoAnn Bomeisl, Manager of Technical Services at the NYS Insurance Department, Marilyn MacBride, Information Security Officer at the NYS Department of Motor Vehicles, Marilyn McCabe, a frequent editor of publications for the Rockefeller Institute of Government, and Gina Marie Smith, Information Security Analyst at the Department of Motor Vehicles, for reviewing drafts of this paper and providing the author, Linda Neidl, with excellent editorial and content formatting suggestions as this paper was being developed. We are also grateful to Ms. Ann McCann, Internship Coordinator at the University at Albany, for her oversight and guidance of this internship project to ensure both its academic and organizational relevance.

A special thanks to the IT Corporate Roundtable for its continuing work with The Forum on business continuity planning and for its support of this research effort.

## Introduction

This paper is part of a series of initiatives undertaken by the New York State Forum for Information Resource Management (NYSFIRM) to assist New York's state and local government organizations with determining their planning needs in light of September 11, 2001 (September 11). It addresses a critical question: *If disaster – natural, technological, or man made – were to strike a facility or network that houses state workers and data, what support exists or is required to secure safe and continued public service to the people of New York?*

Our purpose is to find support for a *continuity planning* commitment in New York State government that assures both the ongoing safety/productivity of state workers and the optimal delivery of critical state services to our constituents during and following crisis. The paper first provides a rationale for continuity planning in the public sector, then defines and distinguishes continuity planning in the context of more familiar concepts and terminology. Following an examination of current legislative and executive initiatives designed to set standards and coordinate strategies for effective planning, we will conclude with a review of current best practices involved in continuity planning phases and offer recommendations for action.

*If disaster – natural, technological, or man made – were to strike a facility or network that houses state workers and data, what support exists or is required to secure safe and continued public service to the people of New York?*

## *A Rationale for Readiness*

State government's responsibility to plan for the continuity of its operations in the face of "a wide variety of disasters" is not a new concept, as the following 1978 legislative finding reflects. However, since that time, profound innovations in information technologies and the devastating events surrounding September 11, have properly sparked renewed concern for just how well prepared we are.

**The legislature hereby finds and declares that a wide variety of disasters, often caused or compounded by mankind's own acts, cause loss of life, property and income, disrupt the normal functioning of government, communities, and families, and causes great human suffering. The legislature further finds that it must provide for preparations to prevent, meet, and defend against and recover from, dangers and problems arising from these emergencies with the least possible interference with the existing division of the powers of the government....The legislature finds that the state must give leadership and direction to this important task of establishing an emergency disaster preparedness program for the protection of each person in the state.**

*NYS Executive Law Article 2B, Disaster Preparedness § 20:  
Historical and Statutory Notes L.1978, c. 640 §7*

First, rapidly emerging technologies have bred increasing interdependencies between and among the private sector and government agencies, leading to an increasing dependency upon those technologies to access, transmit, and store the vital information that is their premier business asset. Technology is changing the way we do business, causing a shift away from stovepipe structures in government toward a theoretically more collaborative and efficient "government without walls."<sup>1</sup> E-commerce and e-government initiatives have taken root, allowing citizens, businesses, and state agencies to become purveyors and consumers of web enabled information flow and transactions 24 hours a day, 365 days a year. Consequently, new business and management theories like business process re-engineering (BPR) and enterprise resource planning (ERP) have called for careful identification and integration of business functions with technology, and for application of critical change management practices to prepare the workforce to meet the challenges at hand and ahead. The very structure of the Internet itself – a self-organizing, decentralized entity born of the military's desire to ensure the survival of valuable information and the continuity of communications during attack – has emerged as an attractive paradigm on the business landscape, challenging old lines of authority with those less tried.

The new dynamic has also bred new risks. For example, a single disgruntled employee has the capacity to sabotage an entire system. Or, the anticipation of unknown disastrous consequences inherent in the Y2K rollover recently mandated costly, deep reaching, cross-organizational planning to identify, address, and mitigate vulnerability from technological failures.

Second, the unprecedented events of September 11 have renewed fear in the American consciousness of the likelihood of enemy attack, a fear that had become much diminished since the demise of the Cold War. Aware that we are vulnerable to unexpected and sudden hits by powerful enemies determined to topple our way of life, we hunger not only to be secure, but also to believe that everything possible is being done in the interest of public safety, or "homeland security." This need to believe we are secure creates secondary vulnerabilities, arising from the creation of false securities purchased by illusions of redress or resulting in victimization by opportunist vendors, as well as potentially restricting the very freedoms "our way of life" celebrates. September 11 and its aftermath opened our collective eyes to knowing that planned, successful, subversive attacks can happen without warning...and because they have happened, we believe it is likely they will happen again. We must be

---

<sup>1</sup> See NYS Governor's Press Release, June 12, 2000. <http://www.state.ny.us/governor/>

ready to successfully mitigate both effects of attack and effects of fear on government business by careful, responsible planning.

Readiness requires that state government be able to continue meeting the needs of its people despite the fear, chaos, and suffering disasters breed. Readiness requires developing a flexible, current, and tested *planning process* in each office, planning that accounts for inventory, alternative communication channels, contingencies, workforce commitment, and understanding of critical priorities. Planning distributes *limited* resources allocated for backed up data, replaced equipment and applications, and the needs of critical displaced, reduced, or disabled personnel. Planning also educates those charged with implementation as to impacts, risks, and remedies. Planning demands support from leadership expressed in terms of time, enthusiasm, and money. This calls for accountability that can only be met because stakeholders and stewards alike believe that preparation of resilient internal operations is a prudent economic practice of the public's business.

## *The Public's Business and Continuity Planning: What's in a Name?*

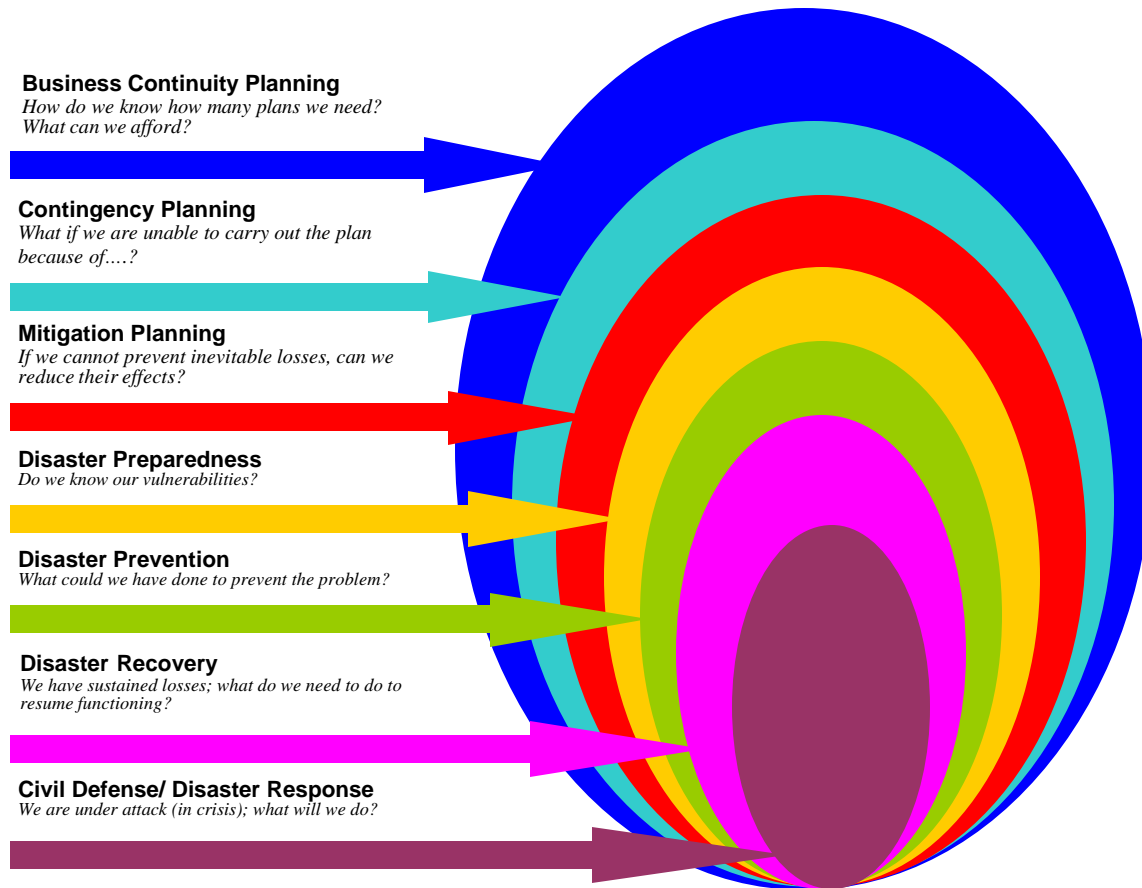
A reader could reasonably ask what has “business continuity” to do with public sector viability. The answer resides in understanding the nature of the “business of government,” distinguishing between continuity planning and related concepts, and assigning appropriate terminology to identify and build the distinct value *business continuity planning* will bring to government operations.

***The public's  
business is  
the public  
services that  
assure the  
public's  
welfare.***

Business continuity planning (BCP) experts predict that “2 out of 5 of enterprises that experience a disaster go out of business within 5 years.”<sup>2</sup> However, unlike the private sector, State governments and their agencies don't go out of business. Discontinuity in the state's ability to conduct the public's business is reflected in lost information, revenue, programs, credibility, and confidence, with increased vulnerability, chaos, and human suffering. The public's business is the public services that assure the public's welfare. If the state is to secure the public's welfare through and after crisis, it must practice a gamut of self-awareness exercises before the crisis that ensure the networks of people, places, and things employed to carry out those services are informed, trained, maintained, upgraded, and enabled to continue operating *despite* disruption, without loss of services essential to constituents no matter how great or small the crisis is. This type of examination of service processes and priorities, coupled with the consequent strengthening of the systems needed to deliver those services, is called *business continuity planning*.

---

<sup>2</sup> Witty, Roberta and Donna Scott, *Disaster Recovery Plans and Systems Are Essential*. Gartner Group. 12 September 2001 [www.gartner.com](http://www.gartner.com). Cited also in Veritas, *Your Data Center Is Down. What's Your Plan?* [www.veritas.com](http://www.veritas.com) 2002.



**Figure 1. Traditional Terms and the Progression of Concepts.** The present phrase *business continuity planning* logically emerges from more familiar terms used for the process of protecting assets, ensuring harmony, and restoring normalcy in the wake of an unplanned, disruptive event. It encompasses the previously entailed concepts, plus ensures that the people charged with carrying out the agency's mission are informed, practiced, and enabled to continue their work with minimal disruption or loss of revenue and service to constituents.

### *The Relationship to Disaster Planning*

Understanding business continuity planning calls for making a distinction about the valued role BCP plays in a family of “planning relationships.” (See Fig. 1.) The “family” is an ancient but still growing body of work – that is, work related to securing the resources an organism needs to survive in the midst and aftermath of a crisis. We might say that BCP is the youngest generation in the family line, a legitimate descendant of such familiar concepts as *good health* or *a fighting chance*. Throughout the millennia, human bodies have developed complex immune systems to fight disease. Through experience, human beings have acquired knowledge of what to do to survive in the face of natural or enemy attack: pull up the drawbridge; batten down the hatches; head for the storm cellar; circle the wagons; quarantine the contagious; fight fire with fire. Survival has always begun with having the right response to a particular threat and the resources needed for that response. Continued survival after the fact has always depended upon an ability to sustain loss and recover function. As learning organizations unto themselves, the fittest survive because they anticipate change and adapt, and business enterprises or state agencies are not exempt from the process.

The generational relationship of the concepts behind the traditional terms is logical and progressive, rather than redundant or interchangeable. The related planning terms, familiarly named

disaster response, disaster recovery, disaster prevention, disaster preparedness, disaster mitigation, or contingency planning, are all from the same gene pool, but BCP comes with some evolutionary improvement, offering a refreshing new skin stretching to bind and protect the “business” from discontinuity. The branches on BCP’s family tree support distinct survival mechanisms by addressing key concerns: *What do we do now? What went wrong? What can we do to prevent the problem? How are we vulnerable? What can we do to reduce the effects of our losses? If we are unable to implement Plan A, do we have a Plan B, or C, or D...?* These questions have been addressed by formulating multiple plans. Business continuity planning encompasses or embraces all the kinds of plans and questions named in Fig. 1, but guides them with an eye on sorting out what resources and services must continue if the public’s critical needs are to be met.

***If continuity is the goal, then the needs of continuity must drive the details of specific choices the organization makes long before discontinuity occurs. BCP in state government seeks to understand what will happen to the agency’s critical services if certain functions are discontinued – no matter what the cause – and measures the risk of loss against the cost of readiness through developing alternative, redundant or resilient resources.***

Business continuity planning is the branch of thought that reasonably addresses *How many plans do we need or can we prudently afford?* It is a layer of thought that could not emerge until after those that preceded it had surfaced; ironically, it now raises questions that must be asked before investing limited resources in any effective planning whatsoever. If continuity is the goal, then the needs of continuity must drive the details of specific choices the organization makes long before discontinuity occurs. BCP in state government seeks to understand what will happen to the agency’s critical services if certain functions are discontinued – no matter what the cause – and measures the risk of loss against the cost of readiness through developing alternative, redundant, or resilient resources. It determines a tolerable level of discontinuity and acts to keep the agency functioning within or above that level.<sup>3</sup> Such understanding requires naming the agency’s mission; naming the business functions critical to the mission; naming the supporting personnel, technologies, and facilities needed to carry out the business functions; naming the impact created by loss of function; naming priorities; and then preparing people, places, properties, and processes to carry out the functions despite failure of “normal” operations. The long shadow of the naming intimates hard choices

about investments and state resources. Business continuity planning is the protocol that navigates the “choice makers” through the shadows.

## Naming

Because business continuity planning is still finding its way into common exchanges around the new millennium water cooler, the term is often misused or misunderstood by and among the stakeholders who have not yet agreed upon its meaning, and consequently, its value.<sup>4</sup> For example, at a recent presentation to NYSFIRM members, Meta Group Vice President Al Passori declared that although disaster recovery commonly refers to technology functions and business continuity is used

<sup>3</sup> For a fuller discussion of this approach, see Herriot, Larry. *Business Continuity Planning Is...* presentation, CDRP, 1997 at [http://www.drj.com/new2dr/w\\_3006.htm](http://www.drj.com/new2dr/w_3006.htm).

<sup>4</sup> We could argue that the ultimate stakeholder is the consumer public whose safety and welfare is compromised by an agency disruption, or the taxpayers who will fund the “to plan or not to plan” consequences. An intermediate stakeholder is the vendor of BCP products and services. However, equally compelling is the argument that the one(s) to blame for the lack of planning have the most at stake; i.e., the IT people, the security people, and the politicians. Compare how Rudy Guliani’s star rose after September 11 because New York City’s plan worked, with the loss of prestige and call for reorganization suffered by the FBI because their intelligence and communication structures did not.

for the work area, the terms are “in reality interchangeable terms.”<sup>5</sup> At a subsequent NYSFIRM seminar dedicated to business continuity, presenters from Empire Blue Cross/Blue Shield, Gartner Group, and Veritas rarely used the billed term, but rather elected to speak of business continuity in terms of a disaster recovery strategy.<sup>6</sup> Along the same line, *Disaster Recovery Journal* advertises itself as “the magazine devoted to business continuity since 1987.”<sup>7</sup> Other industry leaders, however, aptly define disaster recovery as a distinct, narrower term, as but one component of a set of plans derived from and implemented because of an enterprise’s awareness of its vital operational needs in the event of interruptions.<sup>8</sup>

***The advantage is that the plan is the planning process itself, a binding process that casts all other plans in the light of a crucial mindset: continuity of service is critical.***

In short, either the terms are interchangeable, or they are not. We contend that they are not, and use business continuity planning as a broad tag that uniquely identifies the process or protocol needed to prudently develop and implement a *set of cohesive plans* required to maintain the public’s business in the event of an interruption. These cohesive plans are concerned with *any type* of interruption that might cause “asset loss, regulatory liability, service failure, or a damaged reputation with constituents.”<sup>9</sup> The evolutionary advantage in this breakthrough layer of planning is broad and flexible enough to include interruptions that are both unplanned (e.g., September 11, earthquake) and anticipated (e.g., Y2K, relocation, retirement<sup>10</sup>). If *any* discontinuity has the potential for disaster, disaster is averted by developing the strength of the connective tissue that fortifies the agency against the breakdown of critical services. The advantage is that the plan is the planning process itself, a binding process that casts all other plans in the light of a crucial mindset: continuity of service is critical. The individual plans minimally include those shown in Fig. 1, as well as others named business resumption, business recovery, crisis management, security self-assessment, and workforce commitment (See Glossary, Appendix A), but it is their respective and collective binding investment in service outcomes that is wanted. Business continuity planning binds resources to service.

Names do matter. Names identify or validate a presence; they direct our attention to or enhance our ability to perceive nuances and values. If business continuity planning is a name that defines a breakthrough layer of thought, a layer that somehow calls for action distinct from what has been defined by traditional terms, then it cannot be “interchangeable” with those previous terms.<sup>11</sup> The need for *cohesiveness* between business functions and supporting technology, *cohesiveness* between development and implementation of planning decisions, *cohesiveness* between and among agencies – all developed within the boundaries of discontinuity, economy, and ongoing service – is the value correct users of the term want stakeholders to perceive.

<sup>5</sup> Breakfast Briefing on “Disaster Recovery, Business Continuity, and Homeland Security,” May 23, 2002 at Rockefeller Institute for Government.

<sup>6</sup> Business Seminar II at the NYS Convention Center in Albany, August 13, 2002. See presentations at [www.nysfirm.org](http://www.nysfirm.org).

<sup>7</sup> See [www.drj.com](http://www.drj.com). The website offers many articles and links relating to BCP best practices.

<sup>8</sup> See for example Gartner Group at [www.gartner.com](http://www.gartner.com).

<sup>9</sup> See NYSFIRM’s Business Continuity Health Check at [www.nysfirm.org](http://www.nysfirm.org). Also Gartner Group literature, including DPRO-100862 10/08/01.

<sup>10</sup> Succession planning addresses anticipated gaps in the workforce created by the retirement of large numbers of long term, knowledgeable employees. Related anticipated interruptions might occur with changing administrations, retraining a workforce for emerging positions, or relocating operations to a new facility.

<sup>11</sup> See Clippinger, John Henry, editor. *The Biology of Business: Decoding the Natural Laws of Business* San Francisco: Jossey-Bass, 1999. This collection of essays develops the biology analogy lightly used here. Clippinger’s own entry on “Tags: The Power of Labels in Shaping Markets and Organizations,” pp. 67-88, examines the relationship between names (tags) and power to effect change.

Assigning a value to ongoing public service in the face or wake of disruptive events by consistently and appropriately naming business continuity planning as a desired practice is the critical first step for supporting the continuity of the public's business in New York State.

## Whose Job Is It?

New York State must not only build value for continuity of services by correctly naming the protective planning process, it must also name who is responsible for leading the workforce and infrastructure to a condition of ongoing "continuity readiness." The good news is that the conditioned response to the breakthrough layer of thought will not be built from nothing, as much is already in place to lead the effort. The bad news...well, *much is already in place to lead the effort*. Unfortunately, contemporary planning needs will be organized around, within, and throughout several institutions and initiatives competing for a place in an existing state government. The innovative process of continuity planning must be assigned as a clear area of responsibility for which someone or some office will be held accountable.

*New York State must not only build value for continuity of services by correctly naming the protective planning process, it must also name who is responsible for leading the workforce and infrastructure to a condition of ongoing "continuity readiness."*

The architects of a secured continuity will not be surveying a cleared and graded landscape; they will be challenged to rehabilitate a legacy – a legacy in which much and many are quite invested. The sheer size of the government, its departmental structure, the complexities of rigid regulations and laws that govern its own operation, and the political realities of the workforce inhibit effective change management.<sup>12</sup> As the Governor's 1995 Task Force on the NYS Civil Service System reported:

**New York State must contend with the competing interests and requirements of numerous state agencies, labor unions, joint labor/management committees, the State Legislature, the Division of the Budget, the State Comptroller's Office, and the courts; a situation which mitigates against achieving consensus about what changes should be made... Action taken at any point in the system sets off a cascading network of reaction....This makes it difficult to effect change to the system as a whole.**<sup>13</sup>

If change in the system as a whole is difficult, and the breakthrough layer of thought changes the name of the game by which we prepare for the myriad contingencies and crises that threaten the state's ability to continue service during crisis, where will the momentum to effect the change come from? Who is responsible for determining the level of preparedness and setting standards for effective planning? Who is responsible for holding the responsible accountable?

<sup>12</sup> As of April, 2002, the state employed over 191,000 people, many in civil service positions (NYS Retirement Data, posted at <http://www.goer.state.ny.us/workforce/agyinitiatives/oscworkforcedata.html>). By state constitution, the Executive Branch, which employs 175,000 members of the state workforce, is organized into a present maximum of 20 departments, under the theory that this ceiling keeps government more manageable and efficient. However, to accommodate government needs that have emerged since the constitutional maximum was set in 1961, the departments have had to expand by creating numerous subordinate divisions, offices, or agencies to carry out their work. The Executive Department alone is the "parent" of 30 of these subsequent organizations. The senior staff of these departments and their proliferating subdivisions are appointed by the elected governor. In addition, there are thirty-three public benefit corporations statutorily created as "public authorities" rather than as departments or as agencies. They are also governed by politically appointed boards to maintain, manage, and improve New York State infrastructure. Of course, the legislature, as well as the governor, all serve "at the pleasure" of the voting public.

<sup>13</sup> NYS Governor's Task Force on the New York State Civil Service System. Quality Standards/Innovative Applications: Prescriptions for Improving New York State's Civil Service System. a Report. December, 1995. <http://www.cs.state.ny.us/pio/back.htm>.

Several distinct state initiatives are presently charged with developing and maintaining some aspect of protection, response, and/or recovery of state operations in times of threat: the NYS Emergency Management Office (SEMO), the NYS Office for Technology (OFT), the NYS Office of Public Security (OPS), and the office of the NYS Chief Information Officer (CIO). The language of each of their respective charters is broad enough to assign or assume leadership for not only disaster recovery or preparedness, but also in asking and resolving the questions entailed in business continuity planning. Any state agency seeking support for continuity planning should be able to turn to these resources. However, nowhere in any of the founding documents or published missions of these initiatives does the term *business continuity planning* appear. Absent this explicit commitment, finding support for continuity planning from an authorized state body or within the agency is a shadowy search.

***...nowhere in any of the founding documents or published missions of these initiatives does the term business continuity planning appear. Absent this explicit commitment, finding support for continuity planning from an authorized state body or within the agency is a shadowy search.***

### *State Emergency Management Office*

In 1978 the NYS Legislature amended Executive Law by adding Article 2B to address the findings quoted at the start of this paper. The new law provided for the creation of a Disaster Preparedness Commission consisting of the highest ranking officials in 20 key department/agencies<sup>14</sup> (see Fig. 2) from the Executive Branch of the government, as well as the chief fire administrator, three appointees of the governor, and the chief professional officer of the state chapter of the Red Cross (§21.) The commission was charged with the duty of studying “all aspects of man-made or disaster prevention, response, and recovery,” (§21.3a) and with preparing annually “state disaster preparedness plans” (§21.3c) that “keep current...an inventory of programs relevant to...operations during disasters and recovery following disasters.” (§21.3d) The commission is to “provide for periodic briefings, drills, exercises, or other means to assure that all state personnel with direct responsibilities in the event of a disaster are fully familiar with response and recovery plans and the manner in which they shall carry out their responsibilities...” (§21.3h). The law defines *disaster* as “[an] occurrence or imminent threat of wide spread or severe damage, injury, or loss of life or property resulting from any natural or man-made causes, including, but not limited to, fire, flood, earthquake, hurricane, tornado, high water, landslide, mudslide, wind, storm, wave action, volcanic activity, epidemic, air contamination, blight, drought, infestation, explosion, radiological accident, water contamination, bridge failure or bridge collapse.”<sup>15</sup> Interestingly, more recent BCP industry leaders have broadened *disaster* to mean “any event that has a low probability of occurrence but is capable of causing devastating consequences and a high level of uncertainty.”<sup>16</sup>

The functional arm of the Disaster Preparedness Commission is the State Emergency Management Office (SEMO), an operation of the Executive Department’s Division of Military and Naval Affairs. SEMO acts as the coordinating agent between state, local, and federal emergency/recovery responders, and participates in compacts with other states and the federal government (FEMA, NEMA, NESEC).<sup>17</sup>

<sup>14</sup> As of July 2, 2002, legislation in both the Senate and the Assembly has passed providing for the director of the Office for Technology to be added as a member of the Disaster Preparedness Commission. See S06765 and A11594 at <http://assembly.state.ny.us/leg>.

<sup>15</sup> Executive Law Article 2B, §20.

<sup>16</sup> See Gartner Group Scott Porter’s presentation at NYSFIRM’s Business Continuity Seminar II, August 13, 2002, at [www.nysfirm.org](http://www.nysfirm.org).

<sup>17</sup> See FEMA at [www.fema.gov](http://www.fema.gov); NEMA at [www.nemaweb.org](http://www.nemaweb.org). Also, Article 2B was amended Sept. 17, 2001 to enter NYS into an interstate mutual assistance compact among the states. See §29.g.

According to a SEMO spokesperson for the Counsel to the Commission, the emergency preparedness plan is a “never ending document,” always under revision, and in process with its member agencies. He offered, “All state agencies must be ready to continue operations in the face of disruption.” He stressed that in preparation for Y2K, each agency was required to review its *continuity* plan, submit it to SEMO, and have it reviewed by the then OFT Task Force. Each plan was to address the agency’s full operating needs, not just IT concerns, and each agency was required to have a command center and redundant communications. SEMO’s website offers sample Y2K planning documents for various levels of local government, and a link to a sample of a state agency plan.<sup>18</sup> He added that SEMO sponsors various training sessions throughout the year, open to diverse public sector personnel to advance emergency management professional development. These are described on the office’s website.<sup>19</sup> Additionally, the September 2002 Annual Conference promised to address responses to particular threats and hazards and invited representatives of “state agencies” to attend, though the specific terminology of agency or *business continuity planning* is not a published part of the agenda.

**“All state agencies must be ready to continue operations in the face of disruption.”**

**SEMO Spokesperson**

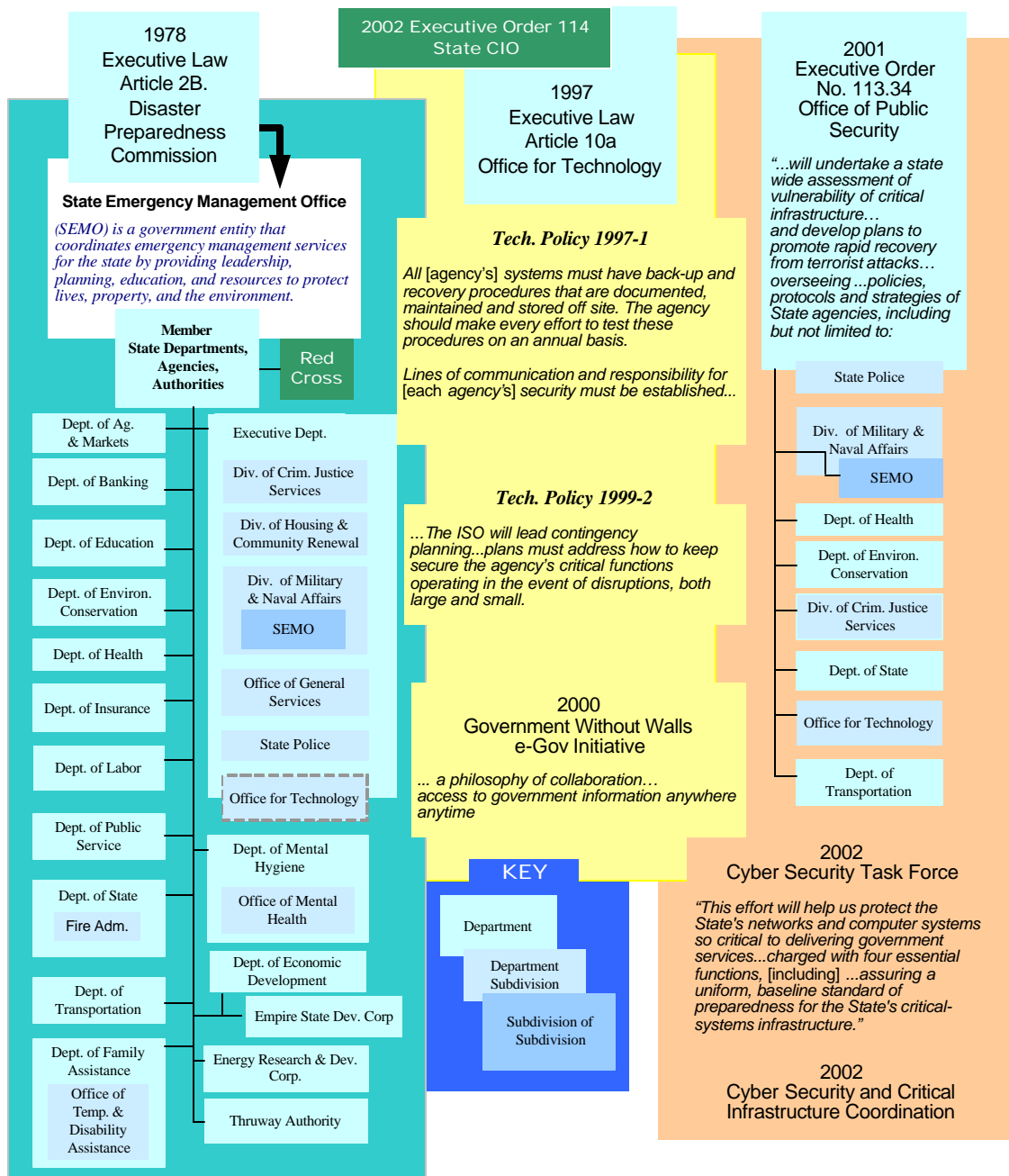
### *Office for Technology*

The Office for Technology (OFT) was created in 1997 under the authority of Executive Law Article 10A as an outgrowth of the Governor’s Task Force on Information Resource Management to “ensure that technology plays a pivotal role in the effective and efficient delivery of state government services...to strategically manage [the State’s] technological resources...Such management must leverage the state’s technology as a vehicle to reform and revitalize government and for promoting positive change.”<sup>20</sup> As defined in the statute, the office’s functions, powers, and duties comprise “establishing statewide technology policies, including but not limited to, preferred technology standards and security” (§206-a(10)) and completing a comprehensive study of the existing state information resource technology infrastructure,” which is to reflect inventories of “existing hardware, software, space/environmental needs, telecommunications and networks supporting operations, and the personnel associated with existing operations and management.” (§206-a(12a-d)). The statute further states that this study is to be completed and submitted to the governor, the senate, and the assembly by October 1, 2002, with interim reports provided in October of 2000 and 2001. By October 1, 2003, OFT must develop and submit confidential, formal disaster recovery plans for the state data center and statewide network, NYe-Net. (§206-a(12-a(d))).

<sup>18</sup> Link now refers user to the OFT website.

<sup>19</sup> See [www.nysemo.state.ny.us](http://www.nysemo.state.ny.us).

<sup>20</sup> See Historical and Statutory Notes L.1997, c.430, §28 for Legislative Intent relative to Article 10A.



**Figure 2. Generations of Protective Initiatives.** Many agencies, offices, workgroups, and task forces are involved in the effort to secure continued services to constituents, but it remains unclear who is responsible for leading New York State in business continuity planning.

OFT's philosophy is to "forge a marriage between agency-specific needs and the best interests of the State"<sup>21</sup> and its work is to make "state government more efficient, integrated, cost-effective and accessible."<sup>22</sup> Because components of technological networks (including personnel) reach deeply into and across all state agencies as a response to agency business needs,<sup>23</sup> OFT is well positioned to champion the integrated continuity planning of business process, technology, and information management in all state offices. Two policies in particular clearly spell out OFT's expectations, which *if* implemented, create a sound platform from which business continuity planning can grow.

First, in January of 1997, the then task force issued Tech Policy 97-1 as a "minimum security policy for the protection of agency assets, including information, computers, and networks." The policy calls for each agency to determine the value of an information asset by "considering...the consequences of unauthorized disclosure, modification, *destruction, or unavailability* of the information. The value of these assets will determine the level of controls needed to provide...backup and access controls." The policy directs each agency to have established lines of communication, with provisions for alternatives, regarding responsibility for information in the "communications chain," and ultimately introduces the need for each agency to have a designated information security officer (ISO). Additionally, "all [information] systems must have back-up and recovery procedures that are documented, maintained, and stored off site."<sup>24</sup>

***...the ISO needs to understand the agency's mission and the relationship of information systems to that mission, must forge cooperative relationships across the agency and with counterparts in other agencies, and lead contingency planning efforts that "address how to keep...the agency's critical functions operating in the event of disruptions both large and small."***

OFT Tech Policy 99-2

Second, in February of 1999, OFT issued Tech Policy 99-2,<sup>25</sup> defining the minimum administrative responsibilities of the agency appointed ISO. The policy states that "The agency must have procedures to prevent, detect, contain, and recover from information security breaches from both internal and external sources and disasters both natural and man made. The ISO has a duty to ensure that these procedures are in place." The policy provides that the ISO needs to understand the agency's mission and the relationship of information systems to that mission, must forge cooperative relationships across the agency and with counterparts in other agencies, and lead *contingency* planning efforts that "address how to keep...the agency's critical functions operating in the event of disruptions both large and small."

The authorized reach of these policies across agency boundaries, when coupled with another OFT charge to "build a government without walls,"<sup>26</sup> is highly suggestive: It would appear that as the new and fastest growing kid on the block, OFT has been invited by the state to teach us a new game to be played with the old

team. The name of the game is *collaboration*, but it will involve a predictable painful reorientation period as the stovepipe players sort out the new rules, build the skills, acquire the equipment, and take their positions.

<sup>21</sup> OFT website at [www.oft.state.ny.us](http://www.oft.state.ny.us). Click on About OFT, then read "Philosophy."

<sup>22</sup> Id. OFT Homepage.

<sup>23</sup> Historical and Statutory Notes L.1997, c.430, §28 for Legislative Intent relative to Article 10A. The note takes care to distinguish that OFT "must fully accept that government programs and services drive technology and not the reverse."

<sup>24</sup> See Tech Policy 97-1 at [www.oft.state.ny.us/policy/tp\\_971.htm](http://www.oft.state.ny.us/policy/tp_971.htm).

<sup>25</sup> See Tech Policy 99-2 at [www.oft.state.ny.us/policy/99-2.htm](http://www.oft.state.ny.us/policy/99-2.htm).

<sup>26</sup> See Pelgrin, William F. *Creating a "Government Without Walls" in New York State*.

[http://www.gsa.gov/attachments/GSA\\_PUBLICATIONS/extpub/10-WFPelgrin\\_2.htm](http://www.gsa.gov/attachments/GSA_PUBLICATIONS/extpub/10-WFPelgrin_2.htm). His article gives a good history and explanation of this initiative and the efforts of OFT on its behalf.

The new position of information security officer, required by the directive from OFT to all state agencies,<sup>27</sup> is one example of the challenges faced in developing a new way of doing old business. There is no official ISO title in the existing civil service lexicon; the policies may spell out duties and responsibilities, but they offer no guidance to qualifications, certification, or compensation. There is no “test” offered to the public or the workforce designed to identify meritorious applicants for the position of agency information security officer. Each agency may have a designated ISO holding the position, but that person may be simultaneously functioning with responsibilities associated with his/her “real” title in addition to those duties bulleted in the ISO tech policies.

Even more complicated is the fact that acting ISOs have emerged from different work pools and are functioning with varying levels of skills and support in their home agencies, while presumably accountable for carrying out OFT directives. As the role and value of electronically generated, transmitted, and preserved information continues to grow, as the partnership between technology and business functions deepens, as public conflict over issues surrounding security, right to privacy, and right to access foment fundamental ethical questions of how we are to govern ourselves as a people, lines of authority get complicated: Who is the ISO and who does the ISO really work for? The same can be asked of agency public information officers (PIO) and chief information officers (CIO).

*There is no official ISO title in the existing civil service lexicon...acting ISOs have emerged from different work pools and are functioning with varying levels of skills and support in their home agencies...*

### *Office of Public Security*

The third candidate for assuming leadership for BCP is the new Office of Public Security, created by Governor Pataki on October 10, 2001 in response to the events of September 11. Under the authority of Executive Order 113.34, the office is to “undertake a state wide assessment of the vulnerability of critical infrastructure...and develop plans to promote rapid recovery from terrorist attacks... overseeing policies, protocols and strategies of state agencies.” The “agencies” specifically named for oversight “include but are not limited to” State Police, DMNA, SEMO, Department of Health, EnCon, DCJS, Department of State, OFT, and DOT. (See Fig. 2 page 9.) Note that the executive leadership of all of these are “members” of the Disaster Preparedness Commission, and already have liaisons “working with” SEMO on an ongoing basis.

All 50 states maintain some type of office as a primary point of contact to coordinate antiterrorism efforts with the federal government. However, New York is one of 19 states that has created a new position, office, or agency to handle homeland security issues since 9/11 in cooperation with the federal office instituted by the Bush administration at that time. The other 31 states have chosen to add additional resources and responsibilities to existing military, emergency management, law enforcement, or public safety structures to meet increased security concerns. In deciding whether to create a new initiative or to assign responsibility to an old one, the states have conducted internal assessments to answer these primary questions:<sup>28</sup>

- ?? *Does our current state structure continuously identify threats and vulnerabilities?*
- ?? *Does our state take corrective action to reduce threats and vulnerabilities?*
- ?? *Does our current organizational structure promote interagency cooperation and information sharing?*

<sup>27</sup> Executive Law 10a §205.4 defines a “state agency” as “any department, board, bureau, commission, division, office, council, committee, or officer of the state. Such term shall not include the legislature or the judiciary.”

<sup>28</sup> See NEMA. “State Organizational Structures for Homeland Security,” [www.nemaweb.org/NEWS/NEMA\\_Homeland\\_Security](http://www.nemaweb.org/NEWS/NEMA_Homeland_Security).

?? Does our state have a capability to respond to and fight terrorist incident?

To accomplish these assessments, OPS has assembled several work groups,<sup>29</sup> most recently the Cyber Security Task Force, a coalition of representatives from state and federal governments, the private sector, and academia. By performing four essential functions, the task force's effort is intended to help protect those networks and systems needed to deliver critical government services:<sup>30</sup>

- ?? Assure a baseline standard of preparedness for the infrastructure.
- ?? Examine vulnerabilities and appraise susceptibility to catastrophic cyber attack.
- ?? Rate and prioritize potential means of cyber terrorism.
- ?? Eliminate redundancy in initiatives and investments.

Like its counterparts in other states, New York's OPS is limited in its scope to terrorist related incidents, and does not assume responsibility for natural or purely technological disruptions. Nonetheless, the scope of information required by and through OPS task forces is relevant, fundamental information generated by and required in the broader BCP process. Any examination of the technological infrastructure done by a workgroup formed with an eye on preparedness, an ear opened to what those who work with the network fear, and a credible voice (and forum) for verbalizing its findings will be operating in the breakthrough layer of thought: *How many plans do we need, and what can we afford?*

### Chief Information Officer

In addition to the anticipated leadership embedded in the three initiatives described above, the power and potential of a fourth very new player excites hope that the hard questions will be asked and that thoughtful answers will matter. On January 28, 2002, Governor Pataki established the position of a state chief information officer (CIO) through the authority of Executive Order 114<sup>31</sup> in response to the growing significance of the Internet and technology in developing state operations, and to further the state's initiatives to create an efficient government without walls. "The order outlines six responsibilities for the CIO, including oversight of the Office for Technology; "Overseeing, directing and coordinating the establishment of information technology policies, protocols and standards for state government, including hardware, software, security and business re-engineering;" and "Coordinating and facilitating information sharing between and among State government"<sup>32</sup>...to promote the use and deployment of information technology that will improve the delivery of government services."

The governor's press release announcing appointment of the state's first CIO stresses the CIO's *coordinating* function and promises that "the CIO will have full authority and responsibility for overseeing, coordinating and directing State resources related to technology policies and resources. These resources are now found in every agency and public authority in New York State."<sup>33</sup>

<sup>29</sup> The workgroups include Law Enforcement, Weapons of Mass Destruction, Public Health, and Cyber Security.

<sup>30</sup> See NYS Governor's Press Release, March 8, 2002 at <http://www.state.ny.us/governor/> as well as NYSFIRM's April newsletter at [www.nysfirm.org](http://www.nysfirm.org).

<sup>31</sup> See <http://www.ofc.state.ny.us/ofc/execord117.htm>.

<sup>32</sup> Per the order, "For purposes of this Order, the term "State government" shall include all state agencies, departments, offices, divisions, boards, bureaus, commissions and other entities over which the Governor has executive power and the State University of New York, City University of New York and all public benefit corporations the heads of which are appointed by the Governor; provided, however, that the powers and duties of the Chief Information Officer shall extend to business and administrative functions of such universities common to State government."

<sup>33</sup> NYS Governor's Press Release Governor Pataki Creates Key State Technology Position, January 29, 2002. See [http://www.state.ny.us/governor/press/year02/jan29\\_1\\_02.htm](http://www.state.ny.us/governor/press/year02/jan29_1_02.htm).

This paper addresses a question: *If disaster – natural, technological, or man made – were to strike a facility or network that houses state workers and data, what support exists or is required to secure safe and continued public service to the people of New York?* We have looked only to the language of the public promises for evidence of a theoretical support for continuity planning. The statutes, executive orders, press releases, websites, and various agency spokespersons all indicate a resoundingly positive implication of “we’ve got it covered” when it comes to asking hard questions and assessing what our state agents need to carry out their respective critical missions during disasters of all types. Nonetheless, a logical series of follow-up questions percolate: Who knows – or needs to know – the answer to the question we raise? Do the words proffered to the public match the reality experienced by those in the public sector workplace? Would acting ISOs read the descriptions written in this paper and say “Not my job” when asked about business continuity planning? Would IT directors sound an alarming “Not happening?” Would a lunch hour interview of random state workers on the Albany concourse reveal a consensus that the promise of preparedness and continuity generates no meaningful response among the rank and file? If there is a gap between what is implied and what is fact, how do we close the gap?

## What's Involved?

The public promises have generated commissions, offices, task forces, workgroups, and executive positions, all filled with people expected to be the actors who implement the hard verbs littering the preceding pages: to *assure, assess, develop, direct, collaborate, coordinate, eliminate, evaluate, examine, identify, inventory, prepare, prioritize, rate, and study*...hard verbs that predicate consequential observations about abstract concepts expressed in terms like *infrastructure, vulnerabilities, missions, resources, worst case scenarios, and preparedness*. If the desired outcome of their collective work is to secure continuity of the public's business in times of crisis, they will need the focus of that goal to guide them as they act. Business continuity planning is an overwhelming, information intense endeavor, requiring input from every office and every worker in the state workforce, input that by its very human nature will not be easily created or handily accepted. Additionally, the integrity of this essential raw ingredient (the input) is crucial, for it is the *catalyst for transformation*. Transformation involves twin investments: investment in gathering input and investment in developing the resources that input names as critical to continuity of services.

Because the outcome (or lack thereof) of the active work potentially affects everyone in the workplace and beyond, under limitless circumstances and unforeseeable degrees of physical, psychological, financial, and environmental trauma, everyone must inform and be informed of the plan. The ownership role of the individual worker in detailing his/her functions, dependencies, and priorities cannot be underestimated, nor can value of the collective understanding possessed by a unit of workers concerning both colleagues' individual work and the units' overall contribution to the agency's mission. Securing quality, consensual input and output during pre-crisis planning secures the cohesiveness and continuity of the organization under crisis. To achieve this, those offering input must believe that their efforts will matter, that recognized and vulnerable priorities will be addressed with policy development, organizational change, and committed funding that make decisive actions viable. This belief will occur and endure only

***Transformation involves twin investments: investment in gathering input and investment in developing the resources that input names as critical to continuity of services. To achieve this, those offering input must believe that their efforts will matter... This belief will occur and endure only with commitments from leadership at the managerial level and from sponsorship at the executive level of government.***

with commitments from leadership at the managerial level and from sponsorship at the executive levels of government.

Best practices in continuity planning carve away the wasted time and resources spent not knowing *Why who does what, where, when, and how*, before, during, and after a crisis. They recognize that BCP is a multiphased process that engages people around information tasks and then generates multileveled group consensus for how the *specific* group can best function to prevent, minimize, or continue despite disruption. Although it promises to minimize the confusion and chaos of uninformed decision making during a crisis, BCP guarantees benefits for all groups who participate in the BCP process whether interruption ever occurs or not: They will emerge with a clarified sense of self as part of a cohesive whole, more aware of their collective and individual assets, and by consequence, provide more reliable public service. The ordinary decisions they make concerning costly purchases of equipment, software, leases, service contracts, professional development, maintenance, meeting schedules, and record keeping will be informed by the goal of continuity. If by its nature business continuity planning is destined to be an ongoing, living “document,” it stands the best chance of being useful if it lives in the minds of those who have to live with it.

### *How It Works*

BCP is a methodology that uses standardized terminology, intuitive sequencing, and a faceted structure to provide flexible but specific guidance capable of accommodating any combination of discontinuity factors. Keeping in mind the costs of public safety, public confidence, and public well-being, at its simplest level, BCP explores and fortifies three facets fundamental to the function of each member of the state workforce in providing service to constituents:<sup>34</sup>

- ?? *How would your work be affected if you were lost or lost access to your work **facilities**?*
- ?? *How would your work be affected if you were lost or lost access to **information/data**?*
- ?? *How would your work be affected if you were lost or lost access to **personnel**?*

Fig. 3 outlines the details and considerations planners must attend to regarding each of these continuity facets.

---

<sup>34</sup> See Missouri at <http://www.oit.state.mo.us/initiatives/business%20continuity.html> and Texas Dept of Info Resources. *Business Continuity Planning Guidelines* at [http://www.dir.state.tx.us/TIC/dir\\_info/dirpubs.htm](http://www.dir.state.tx.us/TIC/dir_info/dirpubs.htm).

	FACILITY FACET	INFORMATION FACET	PERSONNEL FACET
<b>Scope</b>	<i>Spaces, furnishings, equipment, and infrastructure connectivity that facilitate work processes</i>	<i>Data stored in paper and electronic formats that are generated by a work process or required to complete one. Includes the operation of the storage/retrieval system and the storage medium itself.</i>	<i>People who are trained, authorized, and available to perform a work process.</i>
<b>Detail</b>	<ul style="list-style-type: none"> <li>?? Safe, secure work area with lighting and furniture</li> <li>?? Power</li> <li>?? Telecommunications hook-up</li> <li>?? Computers configured with required applications</li> <li>?? Monitors</li> <li>?? Printers &amp; copiers</li> <li>?? Telephone &amp; fax</li> </ul>	All <ul style="list-style-type: none"> <li>?? Files and records</li> <li>?? Databases</li> <li>?? Directories</li> <li>?? Policies, reference resources that inform work procedures</li> <li>?? Instructional materials, forms, and publications for public use</li> <li>?? Web pages</li> </ul> Stored in/on <ul style="list-style-type: none"> <li>?? Paper resources</li> <li>?? Floppies, tapes, CDs, zip drives, hard drives</li> <li>?? Network (server, topology, protocols, security)</li> <li>?? Mainframe</li> <li>?? Inter/Intranet</li> </ul>	Because they possess: <ul style="list-style-type: none"> <li>?? Familiarity with process, including its goals, regulations, and dependencies</li> <li>?? Skill proficiency required to complete the process</li> <li>?? Authorization by title, chain of command agreement, assignment, certification, identification verification, password</li> <li>?? Ability to physically and psychologically function in the design ated position as well as ability to access the facility, information, and other personnel needed to perform the work process</li> </ul>
<b>For each business process, consider:</b>	<p><i>What will we do if the tools we need are unavailable?</i>            Depending on how long we can function without them without intolerable harm, we accept loss or plan for hot site, warm site, cold site, quick ship, and reciprocity agreements.</p> <p><i>Can resilience or replacement be built into product performance or service agreements?</i></p>	<p><i>Where else does the information we need exist?</i>            If the answer is "nowhere" and the information is critical, resources must be allocated to duplicate it and preserve it off site.</p>	<p><i>Who else can do Joe's job?</i>            A list of substitutes must be collected. Or, to the extent that Joe's skills are unique and in high demand, or that his organizational knowledge is broad and deep, investment in succession planning must be made.</p> <p><i>What emotional support might Joe, his family, or coworkers need to aid in continuity or recovery?</i>            Workers who are grieving or concerned about family safety are not free to work.</p>

**Figure 3. Essential Facets of Continuity.** To the extent that the detail of any facet is required in an agency's business process, continuity of the process is compromised when the detail is destroyed or disabled. If the process is time sensitive and critical to the agency's administration or mission, or if the facet detail represents a single point of failure, investment in protecting the process and facet detail becomes more important. If process discontinuity affects public safety or confidence, the highest availability of alternative, redundant, or replacement resources becomes critical.

The values assigned to the facet entailments during the overlapping phases of business continuity planning direct choices that must be made to assure continuity of services. The maps identify what losses of function can be tolerated, prevented, mitigated, worked around, and recovered while mission critical services are continued, lesser mission services are resumed, and “normalcy” is restored. The maps illuminate the gaps; the gaps beg attention; the attention begets action. The phases of BCP enjoy a momentum in a dynamic and cyclic sequence of initiation, development, and implementation of improved practices, each premised on the equation that *Continued operations = Personnel + Information + Facility management*.

### Initiation

The initiation phase of continuity planning combines a series of back-up steps taken to build the momentum needed for getting the undertaking off the ground and keeping it going. It aims to stimulate interest among key players by harnessing credible awareness of existing resources/functions to a credible analysis of risks and potential for harm that can come from not planning for disruption. How far the interest spreads will be reflected in the level of support garnered from leaders and sponsors, who in turn will determine the scope and structure of the planning process. Therefore, the tasks of the initiation phase will include auditing current policies and procedures; inventorying hardware, applications, contracts, and regulations; itemizing services and work products provided by each employee; identifying interdependencies; assessing risks; and conducting a business impact analysis. This information creates a logical springboard for developing a solution-oriented mindset.

***The maps illuminate the gaps; the gaps beg attention; the attention begets action.***

Theoretically, BCP can be initiated by anyone motivated to ask the right questions and capable of creating a willing audience, whether they be superiors, peers, or subordinates. If the impetus originates at lower levels, it must seek the attention of executive sponsorship, whose authority can reach high, deep, and wide into the agency to create teams, establish expectations, and procure the funding needed for the plans' implementation. On the other hand, if the impetus originates at the executive level, it must seek the support of lower level leadership whose familiarity with the people and business functions under study is both specific and influential. Without such support, the executive initiative will meet with resistance and resentment. Input will arrive late, incomplete, and insincere, if at all.

A caveat about responses to information-related initiatives is noteworthy. BCP is not an easy sell, whether it is moving from the top down or the bottom up, but move it must to engage enterprise-wide involvement if it is to be effective. The initiating agent needs to locate and massage the bottlenecks. In general, a push-pull dynamic governs the world of information sharing in any organization of human beings, a dynamic that intensifies as the parties involved are distanced from understanding one another's objective. Information we *push* at others often meets resistance. Our item may be competing with more pressing items for our audience's attention; the terminology may be too unfamiliar or abstract; the format dense or distracting; the content threatening in some way. If we wish to push effectively, we adapt our strategies to identify and minimize the barriers blocking effective reception: change our timing, simplify our presentation, signify respect, accept limitations. Conversely, we ourselves may desire to know certain information, but *pull* at it with great difficulty from perceived resources. The information resources we require may in fact not exist, be unidentified (we don't know where to look), or scattered throughout the organization. We may know that resources do exist and who/what they are, but be unable locate or access them. Or, we may find them unintelligible, unwilling, or unable to meet our needs. These real constraints on the human capacity to absorb, synthesize, share, or create information will be a factor at play in the work ahead, a factor intensified by the political and bureaucratic operations of government. Without sensitivity to factors that govern information related behaviors, pushed directives that inform levels of authority of a need

or requirement to do continuity planning will be ineffective, as will queries trying to pull information from inter/intra-agency resources.

### Low hanging fruit?

- ?? Start where people are invested and generate a climate of concern and resourcefulness. Every employee has a vested interest in his or her own safety and in communicating the value of his or her contribution to the agency's work. Additionally, every employee benefits from believing that others share in and respect those interests.
- ?? Audit and leverage your own awareness of existing emergency or recovery procedures; itemize and prioritize your work functions; inventory your dependencies on applications, equipment, and other people's work. Learn what you can about continuity planning through available resources, and make use of checklists or planning done for Y2K. Use continuity terminology in workplace conversations. Collect/create/copy contact information (e.g., personnel, vendor) you need to do your work and decide where the information will be stored, on and off site.
- ?? Know your sphere of influence and use it to focus attention on prevention, mitigation, response, and contingency opportunities. If in a supervisory position, assist your unit in planning activities and make participation part of performance reviews. Ask peers and superiors what you are supposed to do *if* different situations arise. Network to the extent that you are able and authorized.

### The Business Impact and Risk Analyses

Dual components of the continuity planning process bridge the initiation and development phases: *business impact analysis* and *risk analysis*. If BCP seeks to keep the organization functioning within or above a predetermined level of tolerable discontinuity, the planning must discover *What can/can't we afford to lose?* and *What's at stake if we lose it?* The answers require setting thresholds, which in turn requires knowing the cost of losses and the vulnerabilities they present to the operations. This analysis begins with creating a breakdown of each work unit's business processes, identifying process objectives, interdependent input and outputs, the personnel and facility details involved, time frame flexibility, and projected losses if the process is delayed or failed. Processes are defined as "an area or grouping of business functions focused on the production of specific outputs"<sup>35</sup> and are classified by those who perform them with triaged terms like critical/nonrecoverable, necessary but recoverable at high cost, and relatively insignificant.<sup>36</sup>

The *business impact analysis* (BIA) examines consequences of an interruption to these very specific agency functions or processes caused by any factor that destroys or disables a work area facility, information or information system, or personnel in any combination. (see Fig. 3 page 15.) BIA uses a pre-established metric to calculate the cost of interrupted operations in terms of public safety, public confidence, and public dollars, considering lost revenue and increased expenses (temporary staff, overtime, rentals, travel, replacements), lost productivity (number employees x hours out x hourly rate), and damaged reputation (with constituents, credit rating with suppliers and financial markets).<sup>37</sup> Impact analysis also considers that losses may be immediate or cascading, as losses compound losses when interdependent units and structures fail.

***If BCP seeks to keep the organization functioning within or above a predetermined level of tolerable discontinuity, the planning must discover "What can/can't we afford to lose?" and "What's at stake if we lose it?"***

<sup>35</sup> See Kentucky. 1999 *Business Continuity Planning Process*.

<sup>36</sup> See Oregon. *State Controller's Division Business Continuity Plan, August 2001* at <http://scd.das.state.or.us/bcp/bcp2001.pdf>. Defined criteria is used as a metric for labeling a process as Class 1, Class 2, Class 3, for example.

<sup>37</sup> See Witty, Roberta. Best Practices. Gartner Group [www.gartner.com](http://www.gartner.com).

The study of a process's purpose, requirements, and failure enables those charged with continuity planning to place a value/priority on protecting the process during crisis. This is achieved by understanding the impact of dysfunction in a facet area, and then mitigating the risk by building alternative, resilient, or redundant resources into organizational strategies, practices, and cost of doing business. This information creates a basis for prudently and properly allocating continuity and recovery resources. Windows of required recovery time (recovery time objective, or RTO)<sup>38</sup> can be determined, as can critical recovery points (recovery point objective, or RPO).<sup>39</sup> The breakthrough layer of thought spotlights self-evident priorities for developing flexible, cohesive continuity action plans.

### *Plan Development and Implementation*

Wisdom reminds us that any plan is better than no plan, and that simple plans are better than those too complex to follow. However, the only plans worth having are ones that work. While part of continuity planning may involve intense documentation, the goal of BCP is not to write a book that will sit encased next to the fire extinguisher or first aid kit, awaiting use in some future time of crisis. Plans that slumber in books are not working.

Kenny Klepper, Senior Vice President for Systems, Infrastructure, and Technology at Empire Blue Cross/Blue Shield, testifies with refreshing candor to his experience as a personal and corporate survivor of the collapse of World Trade Center 1. Emphasizing that no worst case scenario prior to September 11 would have ever entertained the events that then unfolded, he recalls the emotional impact and chaos of the evacuation, and allows that grabbing for lists or a "planbook" would not have been on anybody's mind. He admits that Empire – whose 2,000 traumatized, displaced Tower employees lost nine colleagues in the collapse as well as 5 kerabytes of ultimately recovered data that day – had no written plan and does not intend as a "lesson learned" to create such a "written plan." Empire's viability emerged because of what *was already working* for the enterprise. He cited three key conditions that were invaluable assets: an intelligent self-healing network which employed a sonic ring able to reroute traffic when a node was detected as down; a resourceful and committed workforce who were empowered to make decisions and leveraged to act responsively to the needs of the organization;<sup>40</sup> and a history of excellent working relationships with the real estate and supplier communities who were willing and able to quickly assist in locating/equipping temporary offices. Continuity was achieved because the equation of quality *personnel* + quality *information* management + quality *facility* provision had long been inherent to providing customers with high quality service 7x24x365.

***The marathon runner who hopes to cross the finish line has conditioned herself to go the distance long before the starting gun is fired. The successful continuity plan needs muscle, lungs, and heart. What has been done and is being done gives continuity a fighting chance, not what will be done.***

BCP's vitality seeks residence in the mindset and competence of every working employee, in the intelligent resilience of the working technological infrastructure, and in the working cooperation of the facility provider network (i.e., supportive relationships with local community, real estate professionals, financial institutions, reciprocity arrangements, vendors, etc.). There is no BCP product handily indexed to address *What will we do?* if or when any one of a million scenarios plays out. Rather, BCP develops as organizational self-awareness develops, and it atrophies as the self-awareness practices

<sup>38</sup> RTO is the point in forward time when operations must be resumed to avert intolerable loss.

<sup>39</sup> RPO is the point looking backward to where stored information used in business processes must be recovered to avert intolerable loss.

<sup>40</sup> Klepper cited stories of an employee in Albany who with colleagues decided to switch the main domain name server from WTC to Albany, of volunteers who staffed the call center, of nurse case managers assigned to work as advocates and contacts with needy employees and their families.

atrophy. The marathon runner who hopes to cross the finish line has conditioned herself to go the distance long before the starting gun is fired. The successful continuity plan needs muscle, lungs, and heart. What *has been done* and *is being done* gives continuity a fighting chance, not what *will be done*.

That said, the single most important concern the state should have as it engages in continuity planning should be *Is the planning engaging? Does the planning process itself engender vitality in the organization, or deplete it?* Discovery of assets, or the development of assets, is a life giving, not life threatening, undertaking. If resistance, apathy, frustration, or a desire to be satisfied with outsourced or printed output characterize the groans of the drones and decision makers, all are well warned that the planning is not developing at all, no matter how much time, money, or effort is allocated or spent.

### *The Team*

Effective continuity planning wants engaging leadership. Leaders are not people who tell others what to do – they are those gifted spirits who bind others to them to follow. Competence, dedication, eloquence, and clarity of vision bind. The team charged with business continuity planning within the agency must have a capacity for effective leadership, and bring to the table the binding concerns of diverse interests.

The teams assembled as core champions of continuity must be people whose combined personal qualities, knowledge bases, and positions of influence inspire others to follow *from different starting points in the agency's units*. The team cannot be limited to IT staff. The team must be a group of carefully selected individuals chosen by proper authority. These individuals most likely will not share one another's perspective and priorities. Their unifying factor will be a passionate and contagious commitment to ever-improved service delivery to constituents of New York State. They will have a freedom to lead because authority has freed them for leadership, and it is for their leadership effectiveness they will be held accountable. With these essential prerequisite attributes understood, the BCP leadership team should represent IT, human resources, operations, finance, and legal interests, and each team and team member should have access to varied layers of governance within the agency, and to counterparts in other agencies.

***The phasing is fluid.  
Implementation exists as  
decisive actions are taken...  
the phases drive each other  
forward or into the ground  
by the momentum of a  
positive or negative self-  
adjusting feedback loop.  
Keeping the feedback  
positive... is the team's  
tendered duty.***

Developing the means to see and attend to the gaps potentially created by a disruptive event requires support for/from the team both for/from those feeding forward specific input about unit functions and facet performance, as well as support for/from those feeding back authority and funding to address unacceptable risks. The phasing is fluid. Implementation exists as decisive actions are taken, thus initiating another layer of self-awareness as a new facet of performance is integrated and evaluated in the effective operations of the affected service processes. In short, once started, the phases drive each other forward or into the ground by the momentum of a positive or negative self-adjusting feedback loop. Keeping the feedback positive by keeping the feed lines open, the organization nourished, and the "plans" exercised is the team's tendered duty.

### *About "How to" Resources*

The BCP experts all describe a process that looks the same, using similar terminology, phases, checklists, and advice. Every best practice underscores the need for updated inventories, contact lists,

and a business impact analysis. They all underscore the need for executive support, and for aspects of the plans to be tested and updated at least twice a year. BCP develops more than a document in hand; it is an overarching planning process integrated into the everyday decision making and operations of the public's business.

The best practice of continuity planning wants cohesiveness created from a collective commitment to ongoing service despite disruptive events. Supporting reference sources, in the nature of conferences, literature, professional consultants, and software, can testify to those experiences that work. They can inform those seeking support of the scope and structure, the terminology, the possibilities and pitfalls of standard or best practices in business continuity planning and help adjust those practices to the needs of the public's business in particular. They can point to model formats, actual checklists, and sample memos. But they cannot provide, replace, or preempt the natural attitude of enthusiastic resourcefulness that the leadership team itself must bring to the table.

That said, supporting reference sources abound, many advertised or accessible for free, subscription, or sale online.<sup>41</sup> For the reader's convenience, Appendix B provides a reference table concerning some exemplary sites, followed by a list of the sources cited in or used as background for this paper.

In addition, NYS Office of General Services (OGS) Procurement Services Group (PSG) has published a brief contracting strategy for BCP and security, available at the NYSFIRM website. PSG oversees centralized statewide contracts for those commodities, services, and technologies for use by all state agencies, and lists the following vendors as on contract (\*) or under contract development with NYS:

- ?? \*Peregrine (asset management and crises response ) tools
- ?? \*Veritas (storage software solutions)
- ?? Sunguard (comprehensive pre-recovery strategies)

OGS also points out that many "back-drop contracts for IT services provide a vehicle to purchase consultant services which include but may not be limited to '...business impact analysis, continuity of operations....risk assessment....disaster recovery.' " Existing comprehensive service agreements with vendors may already offer the kind of support those charged with leading the BCP process need or are seeking.

## Conclusion

Recent developments in technology and world events have significantly affected our consciousness of the profound risks that exist to the state's ability to continue its service to the public during a wide variety of disasters potentially caused by man-made, technological, and natural circumstances. Planning for all the possibilities has evolved to a breakthrough layer of thought and action: Since we can't plan for every scenario of attack, the eye must be set upon *continuity of services* no matter what the scenario, and all people involved in securing or providing those services must be engaged in the collaborative work needed to achieve that goal. Business continuity planning is a proactive, ongoing self-assessment/self-improvement process that seeks to analyze assets, identify priorities and vulnerabilities, and then calculate potential impact of lost services in order to prudently develop resilience and redundancy in personnel, information management, and facility support. Failure

---

<sup>41</sup> A recent Google search using the keywords *business continuity planning* returned over 375,000 hits. Enhancing the same search words by enclosing them in quotation marks reduced the returns to a no more manageable 20,300 matches, and narrowing them even further by typing "*business continuity planning*" AND "state government" still left an inquiring reader with an overwhelming 3,470 options. Scrolling down the sidebars and reading the extensions of sites listed on the first Google pages confirms that the vendors (.com) want their share of the action in this growing area of expertise, and that the universities (.edu), non profits (.org), and governments (.gov) have their say as well.

in any facet essential for service provision has the potential for creating or cascading disaster. The best way to secure continuity of the public's business is through fortification of the facets themselves, i.e., the personnel, information management, and facility support networks that may face anticipated or unplanned interruptions. Recognizing the cohesive and self-protective value that distinguishes the concept of business continuity planning from other related planning strategies is an innovative way to improve government service to our constituents.

The governor and the state legislature have established several offices, commissions, task forces, and work groups to ensure optimal operations during and after crisis, but explicit state responsibility for business continuity planning is not clear in the present government structure. Surely the newly created Cyber Security and Critical Infrastructure Coordination will play a vital and central role in statewide coordination in the near future. Though continuity planning requires everyone's participation, no one can make it happen outside of an atmosphere fully enriched by interest and investment of a designated, genuinely committed leadership. State agencies should expect to find responsive resources for developing and adapting continuity strategies specific to their own missions and business processes, and know where to find them. Authorities have a duty to support their creations by providing them with necessary resources, including adequate staffing, titles, access, time, education, policy, deadlines, contracts, and technology. These resources may be costly and are not unlimited, and a just distribution can only occur when a careful investigation has determined essential services, and attached them to work processes, available personnel, IT, interdependencies, and impacts if lost. The employment of business continuity planning practices provides cohesive guidance for decision making when it comes to funding, staffing, facilitating, and innovating government operations for safe and continued service to the people of New York State.

**T***herefore, we conclude that three actions are required in order to facilitate the development of a compelling business case and action plan within New York's state and local agencies:*

- ?? The concept of continuity planning must be elevated to a greater priority. The term and function of business continuity planning should be integrated into public policies, workplace communications, professional development opportunities, lines of organizational budgeting, job responsibilities, and performance reviews.
- ?? Clear responsibility for who will lead and coordinate continuity planning must be established, both within agencies, and as an overarching support for state and local government. Cross-organizational leadership teams invested with influential personalities, established program/technical authority, defined titles, and adequate training are required. Technology staff should be part of such teams, but not make up the entire team or represent a disproportionate number.
- ?? Adequate resources must be made available at the agency level to effect an ongoing process of planning, developing, and implementing continuity measures to protect the public's business from intolerable harm and disruption. Necessary resources include funding, contracts, personnel development, possible organizational restructuring, and technological improvements aimed at enabling continuity of services despite any type of event that threatens provision of vital government services.

Visit The Forum's web site ([www.nysfirm.org](http://www.nysfirm.org)) and use the Business Continuity Health Check as a quick way to assess the adequacy of your organization's plans for business continuity.

The Business Continuity Health Check was developed by the Forum's members in conjunction with members of the Forum's IT Corporate Roundtable and is available for use by any organization at no charge.

## APPENDIX A: Glossary

**Business continuity planning (BCP)** – a set of cohesive plans to recover business operations in the event of an interruption that might cause business process failure, asset loss, regulatory liability, customer service failure, or a damaged reputation with constituents. [source: NYSFIRM BCP Health Check. See also Gartner DPRO-100862 October 8, 2001]<sup>42</sup>.

- ?? **Business resumption plan** – to continue mission critical functions at the production site through workarounds until the application is restored.
- ?? **Business recovery plan** – to recover mission critical functions at an alternate site (sometimes called workspace recovery).
- ?? **Contingency plan** – to identify potential internal and external threat scenarios which may interrupt business operations (also called mitigation planning).
  - Per Gartner only: “to manage an external event that has far reaching impact on the business.”
  - Per Kentucky BCP: “a strategy that provides a description of resources, staff roles, procedures, and timetables needed to achieve a minimum acceptable level of output for each core business process.”
- ?? **Crisis management plan** – the process by which the scope of the interruption is determined and the level of response that is needed. This includes communications to employees and constituents to maintain their confidence.
- ?? **Disaster recovery plan** – to recover mission critical technology and applications at an alternative site.
  - Per Kentucky BCP: should include location, contacts, resources, and information vital to disaster recovery. (p. 13)
- ?? **Security self-assessment plan** – a quick check to test the availability and effectiveness of security policy, procedures, education, and culture.
- ?? **Workforce commitment plan** – tests the level of commitment of IT workforce as a predictor of the likelihood of retention problems that could be an obstacle for agencies to get their mission critical work done.

**Business Process** – area or grouping of business functions focused on the production of specific outputs.

**Cold site** – empty office space ready for equipment to be moved in by the customer. [Gartner: DPRO-100862 October 8, 2001] Also, mobile trailer sites and porta-sites.

**Hot site** – “fully equipped, operationally ready data center offering specific hardware ready for almost immediate use when provider is notified of a disaster (office space/furnishings, computers, phone jacks).” [Gartner: DPRO-100862 October 8, 2001]

**Impact analysis** – most basic component of a BCP, it examines the consequences of an interruption to an organization's processes, computer systems, and supporting infrastructure.

**Infrastructure** – the computer and communication hardware, software, databases, people, facilities, and policies supporting the enterprise's information management functions. Also, basic installations and facilities upon which a business depends: specifically, power plants, water, communications, and transportation.

**Risk assessment** – activity performed to identify risks and estimate their probability and impact of their occurrence; used to provide an estimate of damage, loss, or harm that could result from a failure to develop individual system components.

---

<sup>42</sup> See also Kentucky *Business Continuity Planning*: “BCP provides interim solutions to resume mission critical activities in a timely manner, at the earliest possible time, and in the most cost effective manner....must also presume failures of critical components, including business partners and service providers...[must have] a set of contingency plans with a single plan for each core business process and infrastructure component.”

## APPENDIX B: On-line Resources

Category	Name and Address	Comment
Commercial	<a href="http://www.disasterrecoveryworld.com">www.disasterrecoveryworld.com</a>	Directory of both BCP and DR resources. Easy to read proponent of COBRA method (consultive, objective, bi-functional risk analysis); site offers templates, checklists, software, and a bookstore.
Commercial	Business Continuity Planning - An Online Guide <a href="http://www.yourwindow.to/business-continuity">www.yourwindow.to/business-continuity</a>	Detailed outline of the process, rationales, sample communications, and checklists.
Commercial	<i>Disaster Recovery Journal</i> at <a href="http://www.drj.com">www.drj.com</a>  <a href="http://www.drj.com/new2dr/model/bcmodel.htm">www.drj.com/new2dr/model/bcmodel.htm</a>	“devoted to Business Continuity Planning since 1987”  <i>DR International model for BCP table of contents, supported with articles explaining each part of the model. Accessible articles tend to revert to DR and contingency terminology.</i> <b>Access to very comprehensive glossary.</b>
Non Profit	Disaster Recovery International at <a href="http://www.dr.org">www.dr.org</a>	“first formed in 1988 as the <b>Disaster Recovery Institute</b> in St. Louis, MO. A group of professionals from the industry and from Washington University in St. Louis forecast the need for comprehensive education in business continuity. Alliances with academia helped shape early research and curriculum development.”
Non Profit	NYS Forum for Information Resource Management at <a href="http://www.nysfirm.org">www.nysfirm.org</a>	Posts a Business Continuity Health Check; educational conferences.
Non Profit	Public Technology, Inc. at <a href="http://www.pti.org">www.pti.org</a>	Click on Research, then the Terrorism & Emergency Preparedness link to find another link to Researched Current News and Journal Articles on preparedness topics.
Education	University of Pennsylvania <a href="http://www.upenn.edu/computing/year2000/links.html">http://www.upenn.edu/computing/year2000/links.html</a>	List of links on BCP best practices. Y2K product, but information still valuable.
<b>State Governments – Best Samples</b>		
Texas	<a href="http://www.dir.state.tx.us/TIC/dir_info/dirpubs.htm">http://www.dir.state.tx.us/TIC/dir_info/dirpubs.htm</a> <i>Business Continuity Planning Guidelines</i> , Sept. 1999. (172 page pdf file.)	Outstanding, comprehensive mode – includes complete process blueprint, sample forms in appendices, glossary, and sources/reference list.
Oregon	<a href="http://scd.das.state.or.us/scdpub.htm">http://scd.das.state.or.us/scdpub.htm</a> <i>BCP Operating Manual August 2001</i> Revised Oct. 2001. (88 page document).	Outstanding detailed document showing BCP of the Oregon State Controller's Division.
Pennsylvania	<a href="http://www.esp-forum.state.pa.us/c_ontplan/taxonomy/site_index.asp">http://www.esp-forum.state.pa.us/c_ontplan/taxonomy/site_index.asp</a> Continuity Planning Website	Outstanding resource of documents, guidelines, powerpoint presentations.

## APPENDIX B: On-line Resources

Arizona	<a href="http://gita.state.az.us/policies_standards/html/p800_s865_bcdr.htm">http://gita.state.az.us/policies_standards/html/p800_s865_bcdr.htm</a> <i>Business Continuity/Disaster Recovery</i> , Standard P800-S865. Oct 15, 2001. (34 pages.)	Document gives overview of planning process, with each phase having listed deliverables and decision points. Glossary included.
---------	---	---

### State Governments – Articles of Interest

Maine	<a href="http://www.state.me.us/mnewsletter/nov2001/from_disaster_recovery_to_business.htm">www.state.me.us/mnewsletter/nov2001/from_disaster_recovery_to_business.htm</a> <i>From Disaster Recovery to Business Continuity</i> . Bureau of Information Services Newsletter. November 2001. 1 page.	Article summarizes rationale for title statement and announces formation of workgroup to study BCP in Executive Branch of state government.
Minnesota	<a href="http://www.admin.state.mn.us/security.pdf">http://www.admin.state.mn.us/security.pdf</a> Memo of State CIO to Agency heads and Governor. March 1, 2002.	Re: audit of agencies shows lack of BCP. Essential to secure agency assets...promises forthcoming tools to help agencies plan.
Missouri	<a href="http://www.oit.state.mo.us/initiatives/business%20continuity.html">http://www.oit.state.mo.us/initiatives/business%20continuity.html</a> Technology Initiative – 4 paragraphs	Office of Info. Tech raises concern about false sense of security in agencies.
New Mexico	<a href="http://cio.state.nm.us/2001DRPITPlans.pdf">http://cio.state.nm.us/2001DRPITPlans.pdf</a> <i>DR Recovery Guide</i> , June 2001. (5 pages.)	CIO requires updated Y2K plans follow BCP guidelines.
North Carolina	<a href="http://irmc.state.nc.us/documents/approvals/B CMPolicy61.pdf">http://irmc.state.nc.us/documents/approvals/B CMPolicy61.pdf</a> Business Continuity Management Policy, May 2001.	<i>Brief overview of purpose and guidelines for IT BCP management.</i>
Vermont	<a href="http://www.state.vt.us/sao/pages/y2k63099xsum.htm">http://www.state.vt.us/sao/pages/y2k63099xsum.htm</a> Office of the Auditor's 1999 Evaluation of the State CIO's Office.	Negative review regarding state preparedness for Y2K. Interesting and candid sample accountability tool.

## APPENDIX C: Sources Cited

- Arizona, State of. *Business Continuity/Disaster Recovery*, Standard P800-S865. Oct 15, 2001  
[http://gita.state.az.us/policies\\_standards/html/p800\\_s865\\_bcdr.htm](http://gita.state.az.us/policies_standards/html/p800_s865_bcdr.htm).
- Clippinger, John Henry. Ed. *The Biology of Business: Decoding the Natural Laws of Business*; San Francisco: Jossey-Bass. 1999.
- Disaster Recovery Journal* [www.drj.com](http://www.drj.com).
- Federal Emergency Management Agency (FEMA). [www.fema.gov](http://www.fema.gov).
- Gartner Group DPRO-100862 October 8, 2001. [www.gartner.com](http://www.gartner.com).
- Herriot, Larry. *Business Continuity Planning Is...* CDRP, 1997 [http://www.drj.com/new2dr/w\\_3006.htm](http://www.drj.com/new2dr/w_3006.htm).
- Kentucky, Commonwealth of. 1999 *Business Continuity Planning Process*. URL unavailable.
- Maine, State of. *From Disaster Recovery to Business Continuity*. Bureau of Information Services Newsletter. November 2001 [www.state.me.us/mnewsletter/nov2001/from\\_disaster\\_recovery\\_to\\_business.htm](http://www.state.me.us/mnewsletter/nov2001/from_disaster_recovery_to_business.htm).
- Minnesota. State of. *Memo of State CIO to Agency Heads and Governor*. March 1, 2002  
[www.admin.state.mn.us/security.pdf](http://www.admin.state.mn.us/security.pdf).
- Missouri, State of. <http://www.oit.state.mo.us/initiatives/business%20continuity.html>.
- National Emergency Management Association (NEMA). Homeland Security Report  
[http://www.nemaweb.org/News/NEMA\\_Homeland\\_Security\\_Report.pdf](http://www.nemaweb.org/News/NEMA_Homeland_Security_Report.pdf).
- NEMA. "State Organizational Structures for Homeland Security," [www.nemaweb.org/NEWS/NEMA\\_Homeland\\_Security](http://www.nemaweb.org/NEWS/NEMA_Homeland_Security).
- Newcombe, Todd and Minh Carrico. "Taking the Wheel" *Government Technology*, August 2002.
- New Mexico, State of. *Disaster Recovery Guide, June 2001*, <http://cio.state.nm.us/2001DRPITPlans.pdf>.
- NYS Emergency Management Office (SEMO) [www.nysemo.state.ny.us](http://www.nysemo.state.ny.us).
- NYS Executive Order 113.34
- NYS Executive Order 117 <http://www.oft.state.ny.us/oft/execord117.htm>.
- NYS Forum for Information Resource Management. [www.nysfirm.org](http://www.nysfirm.org).
- NYS Forum for Information Resource Management. Business Continuity Health Check. [www.nysfirm.org](http://www.nysfirm.org).
- NYS Forum for Information Resource Management. Business Continuity II Seminar. [www.nysfirm.org](http://www.nysfirm.org).
- NYS Governor's Office of Employee Relations. <http://www.goer.state.ny.us>.
- NYS Governor's Press Release, June 12, 2000 <http://www.state.ny.us/governor/>.
- NYS Governor's Press Release, January 29, 2002 <http://www.state.ny.us/governor/>.
- NYS Governors Press Release, March 8, 2002 <http://www.state.ny.us/governor/>.
- NYS Governor's Task Force on the NYS Civil Service System. Quality Standards/Innovative Applications: Prescriptions for Improving New York State's Civil Service System. A Report. December, 1995. <http://www.cs.state.ny.us/pio/back.htm>.
- NYS Legislature. Executive Law Article 2B <http://assembly.state.ny.us/leg/?cl=39&a=5>.
- NYS Legislature. Executive Law 10a Historical and Statutory Notes L.1997, c.430, § 28 for Legislative Intent relative to Article 10A.
- NYS Office for Technology (OFT) "Governor Pataki Appoints James Dillon as New York State's First CIO"  
<http://www.oft.state.ny.us/oft/cio.htm>.
- NYS Office for Technology (OFT) Philosophy [www.oft.state.ny.us](http://www.oft.state.ny.us).
- NYS Office for Technology (OFT) Technology Policy 97 <http://www.oft.state.ny.us/policy/PolicyBySubject.htm>.
- NYS Office for Technology (OFT) Technology Policy 99-2 <http://www.oft.state.ny.us/policy/PolicyBySubject.htm>.
- North Carolina, State of. *Business Continuity Management Policy*, May 2001  
<http://irmc.state.nc.us/documents/approvals/BCMPolicy61.pdf>.
- Oregon, State of. *State Controller's Division Business Continuity Plan, August 2001* at  
<http://scd.das.state.or.us/bcp/bcp2001.pdf>.
- Passori, Al. *Business Continuity Market Trends and Issues*. Power Point presentation and promotional materials. META Group. [alfred.passori@metagroup.com](mailto:alfred.passori@metagroup.com).
- Pelgrin, William F. *Creating a "Government Without Walls" in New York State*.  
[http://www.gsa.gov/attachments/GSA\\_PUBLICATIONS/extpub/10-WFPelgrin\\_2.htm](http://www.gsa.gov/attachments/GSA_PUBLICATIONS/extpub/10-WFPelgrin_2.htm).
- Pennsylvania, State of. *Continuity Planning Website*  
[http://www.esp-forum.state.pa.us/contplan/taxonomy/site\\_index.asp](http://www.esp-forum.state.pa.us/contplan/taxonomy/site_index.asp). See also Office of Information Technology site [www.oit.state.pa.us/cwp](http://www.oit.state.pa.us/cwp).

## APPENDIX C: Sources Cited

- Texas, State of. Dept. of Info Resources: *Business Continuity Planning Guidelines*  
[http://www.dir.state.tx.us/TIC/dir\\_info/dirpubs.htm](http://www.dir.state.tx.us/TIC/dir_info/dirpubs.htm).
- Veritas, *Your Data Center Is Down. What's Your Plan?* Power Point presentation and promotional materials, 2002.  
[www.veritas.com](http://www.veritas.com).
- Vermont, State of. *Office of the Auditor's 1999 Evaluation of the State CIO's Office*  
[www.state.vt.us/sao/pages/y2k63099xsum.htm](http://www.state.vt.us/sao/pages/y2k63099xsum.htm).
- Witty, Roberta. *Best Practices in Business Continuity Planning*. Gartner Group. [www.gartner.com](http://www.gartner.com).
- Witty, Roberts and Donna Scott. *Disaster Recovery Plans and Systems Are Essential*. Gartner Group. September 12, 2001.  
[www.gartner.com](http://www.gartner.com).

## Background Sources Not Cited

- "Business Continuity: Are You Prepared? Strategies, Products and Services for Today's World." Special Advertising Section of *Fortune Magazine*, May 13, 2002. See also [www.fortune.com/sections](http://www.fortune.com/sections). Click on "Corporate" for the Genuity I and Genuity II articles.
- DRI International. *Standards for Business Continuity Planning Professionals* <http://www.dr.org/ppcont.htm>. Also, *Professional Practices for Business Continuity Planning* [www.dr.org/lib/pp](http://www.dr.org/lib/pp).
- Florida, State of. <http://www.floridadisaster.org/>.  
<http://www11.myflorida.com/inspectorgeneral/reports/10c-6002.PDF> *Business Resumption Plan Audit*
- Gartner Group. *Aftermath: Business Continuity Planning*. September 21, 2001. See Resource ID 341011 at <http://www4.gartner.com>. Enter document title in search window. Related articles and links to presentations available.
- Georgia, State of. *Pre-Disaster Mitigation Program* <http://www2.state.ga.us/GEMA/>. Or, see [www.gema.state.ga.us](http://www.gema.state.ga.us).
- Kreizman, Baum, Keller. *Disaster Recovery: What Governments Should Do Now*. Gartner Group. Research Note 20 September 2001. [www.gartner.com](http://www.gartner.com).
- Massachusetts Institute of Technology. *Business Continuity Plan* [http://web.mit.edu/security/www/MIT\\_Pub\\_Plan.pdf](http://web.mit.edu/security/www/MIT_Pub_Plan.pdf).
- National Association of State Chief Information Officers (NASCIO) <https://www.nascio.org/>.
- National Infrastructure Protection Center *September 11, 2001, Terrorist Incidents Lessons Learned: New Approaches Needed for Disaster Recovery and Business Continuity Planning HIGHLIGHTS*, December 7, 2001.  
<http://www.nipc.gov/publications/highlights/2001/highlight-01-11.pdf>.
- NYS Budget. Financial Year 2002-03 <http://66.109.35.3/dob/pubs/executive/fy0203.pdf>.
- NYS Joint Loss Reduction Partnership Project. [www.nysemo.state.ny.us/Joint/Jlrpprog.htm](http://www.nysemo.state.ny.us/Joint/Jlrpprog.htm). This project evolved into Business Network of Emergency Resources, Inc. at [www.bnetinc.org](http://www.bnetinc.org). BNet addresses the emergency management and communication needs of businesses on a statewide level and offers a cooperation of public/private sector services to that end.
- NYS Office for Technology Strategic Plan. <http://www.oft.state.ny.us/strat/tforce.htm>.
- NYS *State of the State Address*. Governor George Pataki, January 9, 2002 <http://www.state.ny.us/pdfs/sos2002.pdf>.  
Pallatto, John. "Contingency Planning: An In Depth Interview With Today's Top Decision Makers." *Internet World*, May 2002.
- Tucker and Hunter. *September 11: Business Continuity Lessons*. Gartner Group. May 2002.
- Witty, Roberta. *Jump-Start the Business Continuity Plan: A Checklist*. Tactical Guidelines TG 14-5245. Gartner Group. Research Note 21 September 2001. [www.gartner.com](http://www.gartner.com).
- Tangore, Bob and Nonie Manion. *Disaster Recovery, Business Continuity and Other Lessons Learned*. NYS Tax and Finance. Power Point Presentation shown at FTA Conference in Nashville, Tenn. See [www.taxadmin.org/fta/meet/am02\\_sum/tang\\_man.pdf](http://www.taxadmin.org/fta/meet/am02_sum/tang_man.pdf).
- South Carolina, State of. *Emergency Recovery Plan* [www.state.sc.us/emd/library/recovery\\_plan/recoveryplan.pdf](http://www.state.sc.us/emd/library/recovery_plan/recoveryplan.pdf).
- SunGuard Recovery Services. *New Insights Into Business Continuity for Financial Institutions*. November 2001  
[http://www.sungard.com/images/Whitepaper\\_v3.pdf](http://www.sungard.com/images/Whitepaper_v3.pdf).

## **2002-2003 Executive Committee**

**Chair**, Gene Pezdek, *Dept. of Environmental Conservation*

**Vice Chair**, F. Michael Donovan, *State Police*

**Secretary/Treasurer**, Joanne Riddett, *Thruway Authority*

Ric Barre, *Dept. of Civil Service*

James Bell, *NYS Senate*

JoAnn P. Bomeisl, *Insurance Dept.*

Gail Croteau, *Office of Mental Retardation & Developmental Disabilities*

Sharon Dawes, *Center for Technology in Government*

Leigh Favitta, *Dormitory Authority*

Stanley France, *Schoharie County*

Robert Freeman, *Dept. of State*

Christine Haile, *SUNY at Albany*

Cecelia Hamblin, *Dept. of Transportation*

Roman Hedges, *NYS Assembly*

Karl Kelly, *Div. of Military & Naval Affairs*

Robert G. Kelly, *Div. of Housing & Community Renewal*

Paul Maguire, *Office of Alcoholism & Substance Abuse Services*

Arthur Markowitz, *Div. of Budget*

Kim S. McKinney, *NYSLGITDA*

Michael Mittleman, *Chief Information Office*

Paula Moskowitz, *Office of General Services*

Peter L. Poletto, *Office for Technology*

Alexander Roberts, *Div. of Criminal Justice Services*

Paul Shatsoff, *Governor's Office of Employee Relations*

David Walsh, *State Education Department*

Ruth Walters, *Office of the State Comptroller*

Eileen Wierzbowski, *State Education Dept.*

### **Staff**

Gregory M. Benson, *Executive Director*

Rebecca J. Buchner, *Executive Assistant*

### **IT Corporate Roundtable**

Aon Group

AT&T

CGI Management Consultants, Inc.

CMA Consulting Services

Gartner

Hewlett-Packard Co.

Keane, Inc.

Bearing Point

Microsoft Corp.

Oracle Corp.

RSA Security, Inc.

Sybase, Inc.

Veritas Software

# *NYSFIRM*

The New York State Forum for Information Resource Management (NYSFIRM) is a network of public officials and State government organizations concerned with information management policy and technology.

Information is a vital resource for New York State. Agencies of State government have widely adopted information technologies to improve their abilities to meet their responsibilities. These technologies, the information they process, and the people who use and manage them are essential components of modern government. Together they support a wide variety of public services, contribute to economic health and development, help to manage the state's physical infrastructure and the natural environment, and foster educational and cultural development. Public managers in New York State have become increasingly aware of a need to articulate information policies and to improve the management of information resources which support state operations. A mechanism is clearly needed to support an ongoing exchange of professional and managerial experiences, to coordinate efforts involving issues that are common or transcend the ability of a single organization, and to facilitate useful sharing of the State's technological, human and information resources.

It is the mission of the New York State Forum for Information Resource Management to promote policies and practices for effective use and management of information resources in New York State Government.

