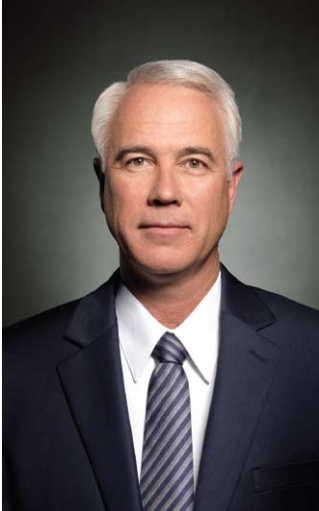


# Resiliency Planning and Continuity of Operations: Beyond Disaster Planning



CIOs are the primary stewards of mission-critical communications infrastructure for government agencies across the nation. Whether it's the ability to keep government operating on a day-to-day basis or managing a multi-agency response to a disaster, communication is the central enabler to getting the job done. Without thoughtful resiliency planning to ensure business continuity, however, communications infrastructure can become the single point of failure for all services.



When government officials talk about infrastructure, they usually mean roads, bridges, water lines, utility plants and other major physical assets. The term “disaster recovery” is rooted in this view of infrastructure.

When CIOs talk about infrastructure, they usually mean systems, networks, applications and other assets that thread through buildings and link various departments, services, command centers and mobile personnel. This infrastructure provides the foundation of daily government operations and economic transactions.

The role of the government IT professional is to continuously and proactively maintain and protect this infrastructure to make vital public services “resilient.” Otherwise what comes after a hurricane, earthquake or explosion might actually worsen the initial event.

Technology is the mechanism to deliver the various systems of government. The CIO’s charter is to build resiliency into the technology infrastructure on an ongoing basis so that the move from daily operations to crisis response is seamless. This can be accomplished through three overarching goals:

- Develop a resiliency planning process that takes an end-to-end view of the region as a holistic enterprise.
- Underscore the unique role of technology and the CIO or IT director within that process.
- Call for a cultural transformation that embeds resiliency planning in the CIO’s daily job responsibilities.

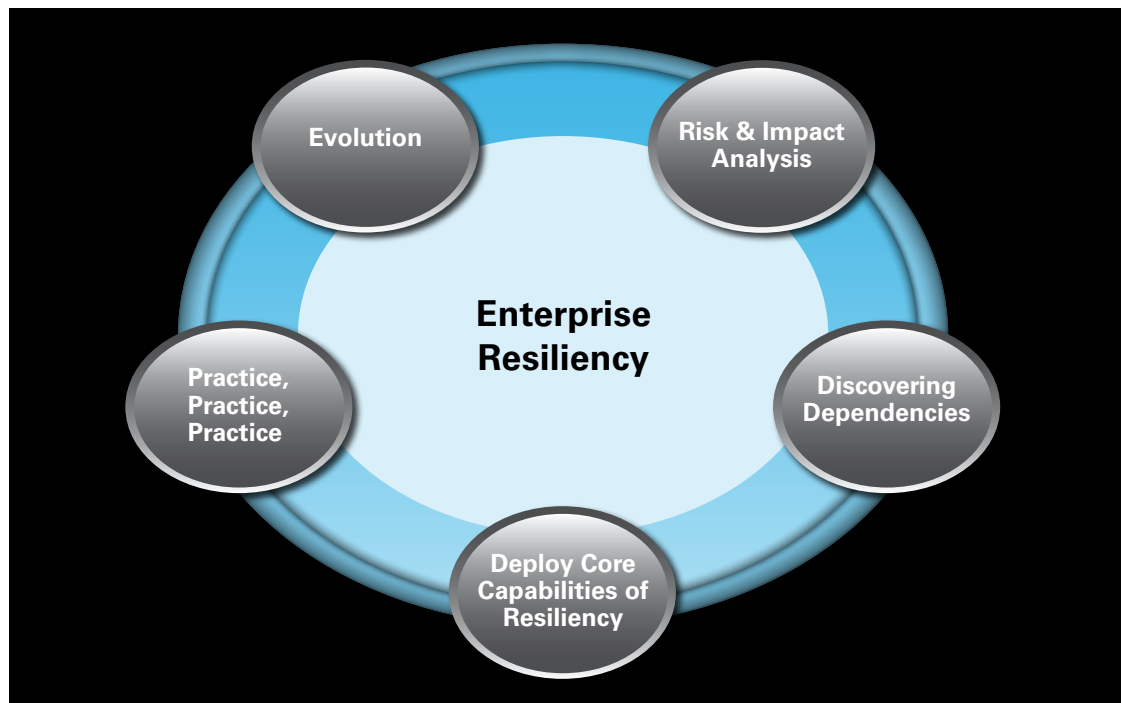
### The CIO’s Role in Resiliency Planning

Technology infrastructure provides the backbone of operational flexibility and the foundation of crisis response. Therefore, technology must fit into a larger plan and the CIO must fight for stakeholder understanding on two different levels – the policy level to make governments aware of technology’s role and what resiliency requires; and the field operational level to drive understanding of what is truly required in a crisis.

Certain items of infrastructure (e.g. key applications, servers, routers, radio networks) must function for anything else to happen. Resiliency planning carries implications for quality of life, economic development and how a community is able to function.

For the CIO, the best technology usage model is one where the technology is so naturally a part of the environment and an extension of the user’s motivations that its usage becomes “second nature,” whether the crisis is a major disaster or a fire in a key facility. This “second nature” philosophy underscores key planning phases, including Risk & Impact Analysis; Discovering Dependencies; Deploying Core Capabilities of Resiliency; Practice; and Evolution

Resiliency planning is a never-ending process. All the technology in the world cannot solve a problem that has not been identified and understood at the levels of daily business, strategic preparation and tactical operations. It begins with honestly analyzing the risks, establishing the priorities and determining where the interdependencies lay.



**Key planning phases of Enterprise Resiliency**

**Phase 1: Risk and Impact Analysis**

The first step is to establish a holistic view of resiliency planning. Agency-by-agency planning is not a holistic process. The city, region, state, or province must be viewed as a complete enterprise and approached with a comprehensive mindset so that true risks can be analyzed and meaningful priorities set. Taking this enterprise-wide perspective also facilitates buy-in amongst political leaders and local businesses as well as helping to break down cultural walls between various agencies. The CIO plays a crucial role in driving this holistic approach.

Resiliency planning starts with three basic questions that form the foundation of a plan:

1. What are the critical services and functions that must survive disaster?
2. What is at risk financially?
3. What is the tolerance for disruption?

Disasters by definition disrupt the normal rhythms of a community. Resiliency planning drives us to identify the rhythms that must be restored quickly and those that can wait. The answers to the above questions form the basis of a plan, but they constitute only the first step in the process. You must now take the list of services and functions required and ask, "Who does that today?" "Who could do it if a backup were necessary?" "Where are my back-up facilities?" "What has to be functional before that service can be deployed?"

**Phase 2: Discovering Dependencies**

Two difficult things must happen in this phase of resiliency planning. First, the owners of functions, assets and public services identified as vital and vulnerable must make tough decisions on what action must be taken to address the vulnerability. Second, all the supporting factors that enable a vital function must be documented, so that interdependencies can be targeted for resiliency assessment.

For the CIO engaged in resiliency planning, protecting systems and network infrastructure requires budget and cooperation from agencies and managers across the governmental and civic enterprise. Strong partnership between the CIO, public safety leaders, and political leaders is critically important. Most importantly, it has to be clear who really "owns" disaster preparedness from a technology perspective. Faced with a known vulnerability, there are only three choices the owner of that priority function can make – fix it; mitigate it; or accept it.

For instance, the information security officer is responsible for the protection of data, including citizen records, business tax records, criminal records, employee personal health information and more. Understanding the risks vs. the investment of enhancing security measures is purely a business decision and the CIO must create an environment in which technical infrastructure is viewed as the basis of service delivery in all circumstances by all stakeholders.



No simple solution exists for a problem that is not understood in its details. This takes us into the realm of dependency chaining – identifying the functions or services that depend on the smooth operation of another service or capability. In charting dependencies, you will no doubt identify interdependencies, singular enablers of multiple services and functions that present single points of failure in a crisis. With dependencies and *inter*dependencies fully documented and understood, you have the framework for a plan. It is time to begin putting tactical considerations into place.

### Phase 3: Deploying the Core Capabilities of Resiliency

Vital functions that support all established priorities must survive the crisis. This requires extensive planning and multiple backup contingency plans. One of these structural interdependencies is communications networks.

Communication is consistently ranked by public safety administrators as their biggest worry in a crisis. Communications networks provide the flow of data for normal functions in daily service delivery and are a common enabling capacity across numerous dependency chains. Conversely, it is a single point of systemic failure in a crisis and an arena where the CIO can make a real difference in the planning process.

Two key communications capabilities that will be stressed in a crisis are the 9-1-1 lines between government authorities and the public and the private voice and data networks that enable first responders to coordinate. Resiliency planning supports these functions and the budgets for ensuring resiliency should be a part of the normal operations, including ongoing maintenance and necessary upgrades required over time.

Likewise, the equipment – from radios to backup mobile sites on wheels – can and should be seen as the normal fabric of governance useful to coordinate civic functions as well as crisis response. Viewing these mission-critical pieces of infrastructure as only useful in a crisis makes personnel unfamiliar with them when lives are in the balance.

The convergence of voice, data and video on these networks creates considerations that must also be understood in advance of a crisis. Redundancy is one strategy toward resiliency and involves the dependency of interoperability.

According to SAFECOM, a Department of Homeland Security agency, interoperability is both a technical and procedural imperative and specifies common communications governance policies to reconcile processes and capabilities. Everyone sharing networks must operate by the same principles. This one compliance point leads to another dependency of common technical specifications for:

- Common communications applications where possible
- Customized interfaces that mask differences between applications
- Standards-based data interchange for pulling and pushing data across disparate networks and systems

These data-oriented rules are just the beginning dependencies for ensuring interoperability. Fixed infrastructure (the first layer of service) might be damaged in unpredictable circumstances. Mobile solutions come in different categories of capability, supplementing and extending fixed capability. Back-up data networks can be established quickly to extend network capability into areas where fixed infrastructure has been damaged or overwhelmed with traffic.

Likewise, CIOs should plan for a stock of critical components (routers, servers, etc.), backup fixed-site command and control centers and mobile command and control vehicles that put the command and control function where it needs to be at a given point in time. One point easily overlooked, however, is that a significant portion of your mobile resources are only useful if they are staged well outside the geographic scope of destruction or an impacted area, in the case of a pandemic.

#### Phase 4: Practice, Practice, Practice

Practice and evaluation are absolutely necessary and must become so ingrained in the holistic enterprise-wide approach that responding to a crisis becomes “second nature.” Yet, this can be one of the most difficult steps for the CIO to build momentum around. Staging a realistic disaster costs money, temporarily redirects personnel from their jobs, and potentially disrupts traffic flows in populated areas. But, it’s important that the CIO and CFO collaborate in making that happen. Investing a little now saves a lot later.

In a city or county, it’s everyone’s responsibility but there must be one owner to make sure it happens. Whether it’s the CIO, city manager, purchasing director, county clerk, mayor, sheriff, or police chief, there has to be agreement that formalizing the plan is only effective if everyone buys into it and practices it on a regular basis. Representatives from various agencies and even key vendor partners must be part of the resiliency planning process and also participate during any disaster scenario. Any exercise should also include a “crisis response center” where all the agency heads, the CIO and critical vendors collaborate and practice the interactions of the response and recovery scenario.

Assuming you have completed this process with open and honest commitment to improvement, you now have a resilient plan. The last step is maintaining resiliency as time passes and changes occur in the regional landscape and halls of power.

#### Phase 5: Evolution

The final steps to formalizing the plan involve:

- Commitment to regular training and practice. Documenting learnings and incorporating them into the resiliency plan.
- Ongoing maintenance and upgrades for all critical networks. Excluding this step means taking on unnecessary risk that can be more costly in the long run.
- Commitment to evolving the plan as time passes and new technologies or new priorities enter the planning horizon.

The resiliency philosophy requires documentation of the stages of response once a situation develops or occurs. Remember, the goal is to minimize risk to people, assets and operational processes. The plan must describe roles, responsibilities, flow of the actions, and be detailed enough to drive action but not so detailed that the script itself becomes a barrier to triggering required activity. Key leaders must have a copy and it must be used and continuously updated.

Part of this documenting process is the determination of who has the authority to trigger the plan’s implementation. Every second counts and hesitation at the outset can have cascading effects throughout the emergency. Leaders must also recognize that cities, regions, states, and provinces are not stagnant. They grow and evolve. New priorities can enter the picture. For the CIO, new technologies can alter dependency chains.

#### **Harris County Secures Interoperable Network**



Interoperability has become an imperative for first responders today but without careful planning, it can introduce new security threats to mission-critical networks. Securing networks, especially interoperable networks, is about more than applying security controls and devices. It involves users, end-to-end applications, and the total environment.

For Harris County, Texas, protecting their radio network and its related technologies meant turning the job over to a trusted partner familiar with managing security in that environment. Harris County called on the Motorola Security Services team to perform a high-level Security Evaluation and Design Service.

Given the size and scope of the network and number of access technologies, Motorola examined all interconnection points for potential security weaknesses, identifying vulnerabilities that could lead to system outages, as well as exposure of sensitive government data and communications.

“The Motorola team provided a straightforward look at our vulnerabilities and recommended actions,” says David Dodson, Division Chief, Harris County Regional Radio. “The information was delivered supportively rather than as criticism, encouraging us to take the necessary steps to further secure our already reliable system to maintain it as a rock-solid network for the future.”

## Motorola can help CIOs strengthen resiliency planning

Resiliency is the capacity to ensure that vital services survive in a crisis. The CIO is uniquely positioned to drive resiliency as an approach to crises because of technology's capabilities to collapse time and space and connect disparate systems and processes. Of the planning stakeholders, the CIO is the one most comfortable with such a core capability of infrastructure and can be a force for bridging cultures, agencies and functions. But doing it alone is often not feasible and Motorola can help.

For over 80 years, Motorola has developed technology designed to help governments focus on the mission, not the technology.

From deployable communications and interoperability to wireless broadband and field mobility, Motorola has developed, built and deployed solutions that enable disaster readiness and recovery. Whether it's additional communications equipment when systems are unavailable, interoperability across multiple jurisdictions and agencies no matter what network they use, or providing enhanced voice and data capabilities to speed access and sharing from the scene to the command center(s), Motorola is your "go-to" partner to minimize risk and get the job done.

Motorola also provides a complete portfolio of services, including those that can help you develop resiliency planning by identifying issues such as obsolete infrastructure, network silos, outdated strategic plans, incomplete characterization of internal processes and lack of appropriate technical skills. In addition, Motorola's end-to-end services can help ensure the physical security of your radio sites, as well as network security that protect your voice and data networks. And Motorola Services can help you strengthen your network for greater redundancy to ensure operational continuity throughout your organization.

For more information on resiliency planning, see "*CIO Leadership for Cities and Counties – Emerging Trends and Practices*" (Published by Public Technology Institute ISBN 978-1-4392-4078-6).



**MOTOROLA**

Motorola, Inc.  
1301 E. Algonquin Road  
Schaumburg, Illinois 60196 U.S.A.  
[www.motorola.com](http://www.motorola.com)  
1-800-367-2346

The information presented herein is to the best of our knowledge true and accurate. No warranty or guarantee expressed or implied is made regarding the capacity, performance or suitability of any product.

MOTOROLA and the Stylized M Logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.  
© Motorola, Inc. (0910)  
RO-99-2215