FOUR POINTS TECHNOLOGY

RSA

A Holistic Approach to Government Continuity of Operations:

The Evolving Threat Landscape and Best Practices for Automating your Continuity of Operations Plan

WHITE PAPER | APRIL 2014

EXECUTIVE SUMMARY

Today, leadership must address multiple physical, cyber, environmental and operational threat vectors any of which alone or in combination can jeopardize the ability of their organization to perform its mission. Internal systems, processes, and personnel are dynamic and the threat is constantly changing.

To counter the contemporary threat environment, government agencies at all levels – federal, state, and local – need more than cybersecurity strategies, fire escape drills, and communication trees for bad weather. This piecemeal approach will certainly stop specific threats, but it limits protection to a few specific situations and fails to take a comprehensive view of all that can interrupt critical work.

A growing number of agencies are taking a comprehensive, all-threats approach called Continuity of Operations, or COOP. COOP is an approach that anticipates a wide range of risk possibilities, establishes sound governance for mitigating them, and ensures an always up-to-date plan that accounts for changing circumstances ranging from new missions to relocated offices. Just as importantly, COOP keeps the agency in compliance with the broad range of Federal regulations and directives.

Based on a recent Govloop Survey, Four Points and RSA have developed this white paper to detail the changing threat landscape that faces our Federal Government and compiled a list of best practices to help your agency automate Disaster Recovery/Continuity Operations Plans (DR/COOP).*

** To see survey results go to www.4points.com/RSA*

The Threat Environment

Threats to an Agency's ability to perform its mission can be physical or cyber, operational, environmental, or organizational. A political impasse forced an interruption of Federal government operations for 16 business days last year. This was a once-in-a-generation event few believed would actually occur. Estimates of the cost of the shutdown vary, but one report put it at between 0.2 percent and 0.6 percent of the gross domestic product for the quarter in which the shutdown occurred. That equals as much as $6 billion in lost output. The cost to the government itself was also high in terms of dollars, performance, and reputation.

The shutdown was not the result of sabotage, subversion, or a cybersecurity attack, but it did show that threats in the broadest sense come from anywhere or seemingly nowhere at all. The Federal executive branch had one advantage in the shutdown: the event was predicted. Administrative leadership had time to make plans so that everyone knew what to do when the closure started.

This advanced warning was not the case at, say, the U.S. embassy in Kabul, Afghanistan, the site of repeated bombings and rocket fire aimed directly at the embassy and the surrounding neighborhood. The National Security Agency did not receive advanced warning when an insider cyber breach resulted in the public disbursement of thousands of secret documents with the potential to cripple the agency's ability to carry out core missions.

Public sector organizations face a long and growing list of threats to the safety of their employees, continuity of their operations, and their reputation and legitimacy. Additionally the online, 24 x 7 nature of business has, if anything, heightened constituencies' expectations of the availability of government services.

Agencies Need a Comprehensive, Dynamic, Automated Approach to the Threat Environment

Government entities, like their private sector counterparts, operate in both physical and cyber spaces. These two domains may be different, but they are connected. Behind every online service is a physical complex system of networks and servers. Behind every office and field employee is a supporting IT function.

A comprehensive business continuity management plan takes into account all the complexity of the threat environment.

- Physical security requirements were made clear in last year's tragic Washington Navy Yard shootings, but physical security also requires attention to fires, floods, and structural failures– anything that can cause injury or death to people within a facility. Weather or other external events can also cause loss of access to offices, forcing the need to invoke alternative work plans. Hurricane Katrina flooded numerous government offices including a nationally used Federal data center.
- Cybersecurity has both external and internal vectors. External threats include cyber attacks and the introduction of malware via increasingly sophisticated phishing. Inside threats come from trusted people acting either in a malicious manner, or simply making mistakes and inadvertent failures like loss of devices or credentials, or accidentally downloading malware. Motivations for malicious operators include simple embarrassment of the organization, disruption of service, or theft of data.
- Policy and compliance risks stem from employees inadvertently or deliberately failing to follow such mandates as the Federal Acquisition Regulation, Competition in Contract Act, Anti-Deficiency Act, the Federal Information Systems Management Act, and agency-specific regulations. Many of these have similar mandates at the state and local government level.

The latest versions of two Federal policies – the National Infrastructure Protection Plan and the Framework for Improving Critical Infrastructure Cybersecurity – both stress the need for strong organizational risk management processes. They emphasize the need for tailored approaches, in contrast to one-size-fits all.

Dynamic Threats Demand a Dynamic Response

Awareness and response are crucial to an agency's COOP, but planners must also engineer responses that give their agency a third and crucial element – resilience. Resilience implies the ability to respond quickly and in such a way as to ensure continuity or minimum recovery times. For example, one response to a cyber threat is to shut down the affected system or cut off access. Such a response may contain the threat itself, but it fails to provide the resilience to avoid more than a brief interruption of online services to employees or constituents.

RSA defines COOP in this way: "A holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause. COOP provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of key stakeholders, reputation, brand and value-creating activities."

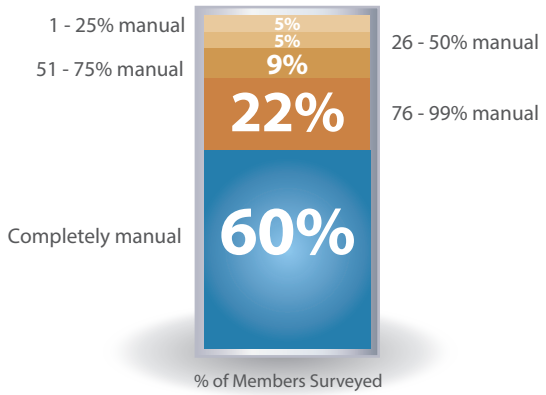
That is, a COOP plan must incorporate responses to possible threats the agency might face and overlay them with three elements required for resilience: governance, risk management, and compliance.

Governance ensures all of the stakeholders are accounted for and that everyone operates off the same playbook in an unlikely event. Risk management prioritizes threats and recognizes that

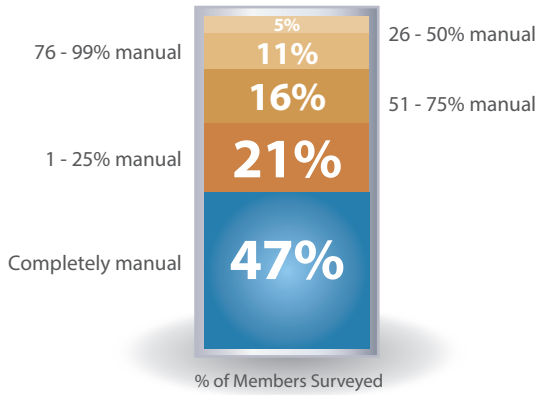
EXPLORING MANUAL & AUTOMATED COOP PROCEDURES

Four Points, RSA, and GovLoop survey of 200+ Federal agency managers about their COOP policies and procedures.

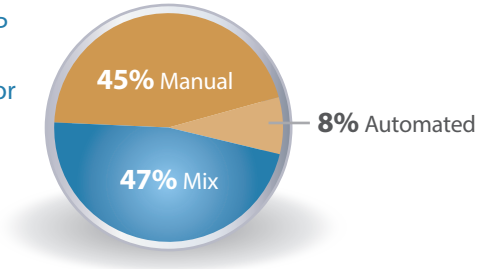
How much of your COOP process is manual?



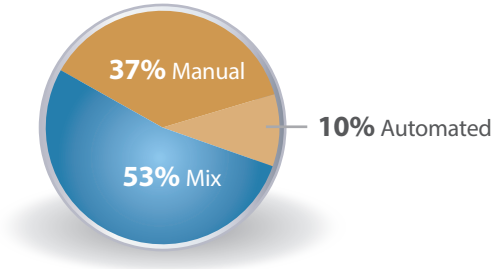
How much of your COOP process is automated?



Is your COOP testing plan automated or manual?



Is your COOP program automated or manual?



Employees Are Mobile. The COOP Should Be Mobile.

Mobile computing has come to government in a big way. Enabled by a new generation of software and a "cloud-first" policy, mobility boosts productivity and improves agency resilience by letting people work anywhere even if offices are unavailable. Therefore, access to business continuity plans must also be available on mobile devices. **RSA Archer BCM Mobile makes this possible.**

The app is available for iPhones and iPads and allows users to see continuity plans and their own required actions. RSA Archer BCM Mobile includes calling tree information to aid communications and it even gives offline access to encrypted data.

not all threats are equally likely to happen. Compliance ensures the agency operates within laws and regulations even when it invokes the continuity plan. For instance, the requirement to protect personally identifiable information or intellectual property is not nullified if the IT staff must suddenly switch to a failover data center.

Because of the high level of dependence organizations have on information systems, IT and data center protection will be an important part of any COOP plan. The plan must incorporate risk to all physical locations and key suppliers, while also having the flexibility to change as missions and other agency parameters change.

Above all, a COOP plan designed to support resiliency must not become a set-and-forget exercise, but rather a living document. The organization must regularly test the plan to know for sure it is up-to-date and relevant with current conditions, and not just responding to the conditions from a month or year ago. Denise Harrison, the CIO of Four Points Technology, LLC, cautions that one pitfall too many organizations stumble into is "lack of diligence of testing the plan which must occur regularly to ensure relevance and execution of the plan so there are no mis-steps when a real event occurs."

Four Points and RSA, The Security Division of EMC, recently retained GovLoop to survey more than 200 Federal agency managers about their COOP policies and procedures. Two thirds said automation of COOP workflow and update processes would be beneficial to ensuring everyone has access to the latest version and all concerns are expressed in future updates.

Other best practices the group identified include conducting business impact analyses of potential interruptions, regularly testing and updating COOP plans, establishing centralized COOP and disaster recovery management while staying adaptable to granular changes in requirements or threats. Shockingly, fewer than half the respondents say they actually follow these best practices.

A Resilient COOP Plan Requires a Flexible Tool

An agency's mission, policies, assets, and people are all subject to risk; therefore, you need an approach to COOP that incorporates all elements in a flexible manner. Because agency mission, policies, assets, and people are all subject to risk, agency leadership needs an approach to business continuity management that incorporates each of these elements in a flexible way.

Among its principal objectives, COOP should let agency stakeholders:

- Develop strategies for both lines-of-business and mission-related processes as well as IT system operations during an incident and plan for recovery after the incident has passed.
- Give employees the information and training they need to respond according to the plan and operate effectively during a crisis.
- Regularly test and refine the plan.
- Incorporate into the COOP governance, risk, and compliance.

The RSA Archer Business Continuity Management solution is a 3-in-1 set of tools designed to let public sector managers build a holistic, enterprise-oriented COOP plan, develop IT disaster recovery plans and manage crisis events. It may be possible to conduct COOP manually, but that approach has many drawbacks. The manual approach typically results in stovepipe plans for each business domain, often in scattered physical locations or on different servers. The manual approach lacks integration, meaning an update to one component will not be reflected in the others. Above all, it fails to provide management a single, holistic view of the agency's COOP. By contrast, a comprehensive tool maintains all of the policies, procedures, and communication plans in a single, central repository.

Because compliance is an important part of COOP, the COOP development software must support Federal and international standards. These include the COOP standard itself, ISO 22301. ISO 22301 is an umbrella standard for a series of sub-standards under development including video surveillance, mass evacuation, emergency management, and public warning. ISO 22301 brought together and unified COOP standards from several nations. Compliance with 22301 proves to legislative oversight committees, executive branch regulators and constituents that the agency practices state-of-the-art COOP.

CONTINUITY OF OPERATIONS BEST PRACTICES

The RSA Archer BCM solution enables compliance with the COOP procedures set forth in the National Institute of Standards and Technology Special Publication 800-34, Contingency Planning Guide for Federal Information Systems. This document calls for a policy and governance framework under which agencies develop business impact analyses, prevention controls, and mitigation strategies. SP 800-34 also specifies methodologies for training, plan testing, and maintenance.

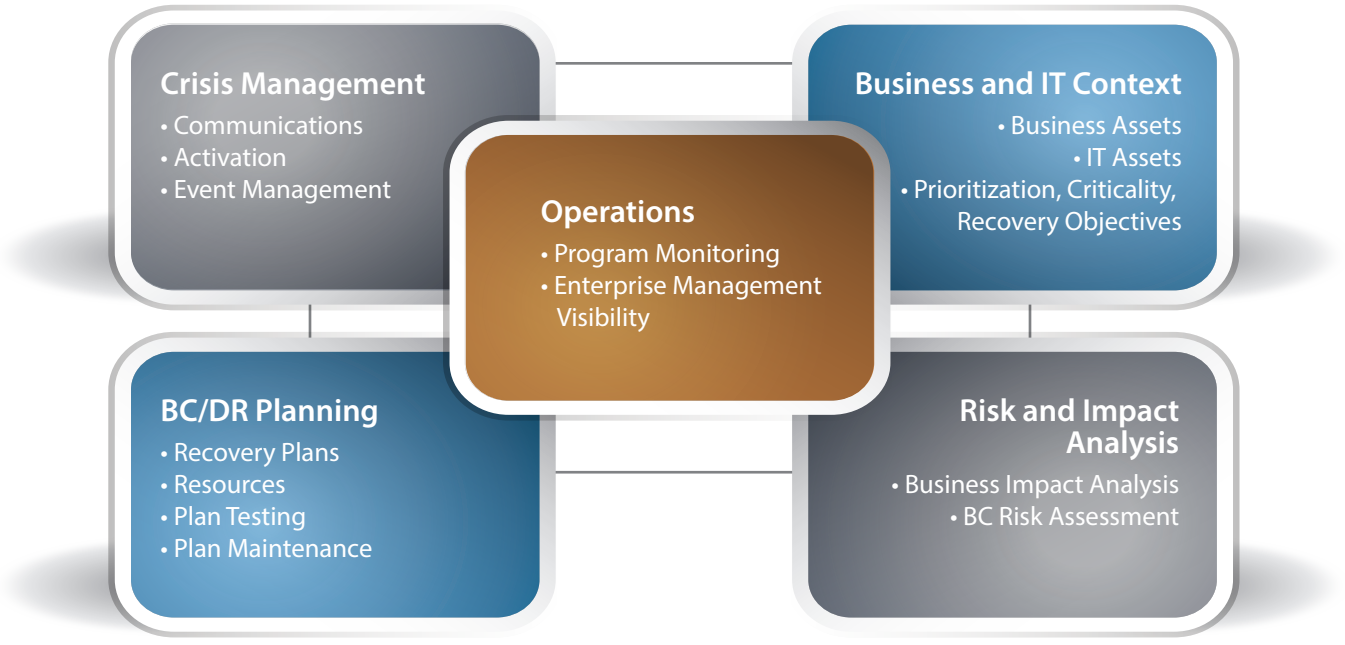
Integration, Ease of Use Are Crucial To Creating a COOP

The Archer toolset consists of a cluster of modules covering the elements of COOP – policy, risk, compliance, vulnerability, and enterprise management. You choose the relevant modules and create a customized plan without the need for coding. Plus, creating a complete COOP plan is fast because of Archer's intuitive user interface and drag-and-drop building.

Archer is among the highest rated offerings in the Gartner Magic Quadrant* for COOP software, both for its completeness of vision and ability to execute. Archer receives high marks for the degree of integration of the specific COOP modules with the larger governance, risk and compliance (GRC) platform.

** Witty, Roberta J. and Morency, John P. "Magic Quadrant for Business Continuity Management Planning Software." Gartner, 26 Aug. 2013.*

CONTINUITY OF OPERATIONS: A HOLISTIC APPROACH



Conclusion

More than ever, public sector managers need to understand the risks and take steps to mitigate them. Good stewardship requires a comprehensive, flexible, and dynamic business continuity management plan, one that results in organizational resilience. Perhaps the most compelling case for a strong COOP solution is the manner in which it achieves enterprise integration to encompass people, systems, policies, and processes. This trend is evident in a number of initiatives. For example, Federal agencies are under a White House mandate to focus on achieving overarching performance goals tied to their mission. Achieving the goals requires an enterprise approach to those same elements – people, systems, policies, and processes. It stands to reason that COOP plans for an agency should integrate them. Moreover, the exercise of creating a COOP execution plan often reveals new and previously unknown interdependencies.

Agencies can no longer afford to rely on manually created, stovepiped, and fixed plans. No one can predict when a potential threat will become a real event, but taxpayers, oversight agencies, and legislators will expect fast, comprehensive responses and a quick restoration of services after an interruption. Delivering that level of response requires use of an enterprise grade toolset in skilled hands.

About Four Points

Four Points Technology, LLC is a CVE-verified Service Disabled Veteran Owned Small Business (SDVOSB) delivering technology solutions to our Government customers around the world. We partner with top manufacturers and software companies to provide our customers with leading edge information technology solutions. As a Federally- focused prime contractor, Four Points Technology offers a strong contract portfolio that includes Government- wide contracts such as GSA Schedule 70 and SEWP IV as well as multiple agency-specific IDIQs and BPAs. Our disciplined approach to the management of product delivery and ancillary services provides access to the latest technology in an environment that supports rapid implementation, clear productivity gains, and short ROIs. www.4points.com

About RSA

RSA, The Security Division of EMC, is the premier provider of security, risk and compliance management solutions. RSA helps government agencies solve their most complex and sensitive security challenges. These challenges include managing organizational risk, safeguarding mobile access and collaboration, proving compliance, and securing virtual and cloud environments. Combining critical controls in identity assurance, encryption & key management, data loss prevention, continuous network monitoring, and fraud protection with industry leading eGRC capabilities and robust consulting services, RSA brings visibility and trust to millions of user identities, the transactions that they perform and the data that is generated.

With RSA's Business Continuity Management and Operations solution, organizations can deploy a holistic management process to prepare for possible disruptions to business processes, manage crises and manage risks to business operations. Organizations can automate their approach to business continuity and disaster recovery planning, and enable rapid, effective crisis management in one solution. www.rsa.com/grc

FOUR POINTS TECHNOLOGY
14900 Conference Center Drive
Suite 100
Chantilly, VA 20151
www.4points.com

email: sales@4points.com
O 703.657.6100
F 703.657.6135
GSA GS-35F-0553P
SEWP NNG07DA16B