

CONTINUITY PLANNING

We view continuity planning as a process of identifying the threats and risks to an organization and defining the adverse impact they pose to the organization's critical operations and/or mission essential functions, which serve as the basis for developing and implementing actions to strengthen organizational resilience.

There are a number of standard methodological approaches governing business and government continuity planning and we thoroughly understand them. The most common are the standards issued by the Disaster Recovery Institute International (DRII) and the British Continuity Institute (BCI), which have traditionally been used to guide the development of private sector Business Continuity Plans, and the U.S. Department of Homeland Security guidelines, defined in Federal Continuity Directive 1 (FCD 1), Federal Executive Branch National Continuity Program and Requirements, that generally guide the development of Federal, state and local government Continuity of Operations (COOP) Plans.

Continuity planning has always been a part of national security planning and is generally recognized as a "good business practice". Continuity planning (or the lack thereof) directly impacts an organization's ability to carry out its critical or mission essential functions under adverse conditions and protect its knowledge, processes, intellectual property, brand, management competence and other elements that may impact an organization's bottom line.

Members of our BCEP Team have proven experience (tested over and over again) in times of peace, war, disaster and national emergencies) in:



- Developing continuity plans for a very wide variety of private and public sector organizations, including a number of Cabinet-level departments and agencies
- Pioneering the development of current Federal Executive Branch continuity programs and the Nation's first comprehensive National Continuity Implementation Plan
- Developing, resourcing, training and exercising continuity teams, be they COOP Emergency Relocation Groups (ERGs) or other staff responsible for executing critical operations
- Designing, developing, conducting, facilitating and evaluating a wide variety of tests, training events and exercises to determine the extent to which continuity programs, plans, policies, procedures, teams, communications, other information technology systems, and facilities.
- Building successful business cases for strengthening continuity programs, obtaining additional funding, and acquiring alternate operating facilities to meet unmet needs.

We believe that business continuity plans, policies and procedures are one thing (a necessary thing); but what really matters is making sure that everyone in the organization understands the plan (and their relationship to it) is what truly makes the plan viable and executable at the drop of a dime; this is the wisdom that drives our collective approach continuity planning. We

Cage: 4RLJ8
DUNS: 169242760
GSA: GS35F0322U Schedule 70

SBA-certified 8(a)
Minority Woman-Owned
SDB

know how to focus on what counts. We help organizations build demonstrable and enduring continuity capability and capacity.

DISASTER RECOVERY PLANNING

When the lights go out, how much time do you have before critical systems need to be up and running to support continuity of critical operations and mission essential functions?

Disaster recovery planning tends to focus on managing and mitigating risks to information technology (IT) and was once considered almost exclusively a data processing function related to the technical recovery of mainframe computers. Today IT disaster recovery involves a variety of policies, processes and procedures designed to protect an organization's data and IT infrastructure in the event of a disruptive situation. Disaster recovery planning has become an increasingly more visible priority in recent years.

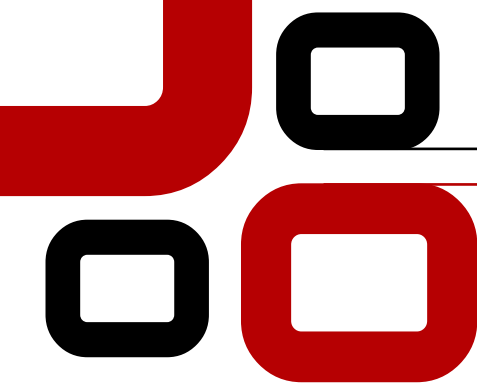
It is estimated that most large companies spend between 2% and 4% of their IT budget on Disaster Recovery Planning, with the aim of avoiding larger losses if continuity of IT infrastructure cannot be assured in an emergency or disaster. Of companies that have experienced a major loss of business data, nearly 40% never reopen, and nearly half close within two years.

While industry and government are better prepared than they have been in the past, the truth of the matter is that the stakes are much higher than ever before. Our nation has never been so dependent on so many disparate technologies, any one of which, if compromised or disrupted, could potentially cripple an organization. Disaster Recovery Planning isn't an option today—it's a necessity and part of doing business in the modern era.

Although disaster recovery planning is largely dependent on technology, our team also focuses on employees and the critical roles they must play when disaster strikes. Recovery and continuity success is largely determined by employees—how they react, how they've been trained, and whether they can put to use the tools they've been provided. Comprehensive Disaster Recovery Planning includes assigning employee roles and testing them on these roles frequently. Employees should know exactly which area of recovery they are expected to focus. The Nova Datacom BCEP team's certified disaster recovery professionals can help business and government strengthen their technological resilience by developing disaster recovery plans, policies, procedures, teams, training, systems and facilities that ensure data centers, critical IT applications, systems and networks, and other IT infrastructure are recoverable within specified timeframes when disaster strikes.

Private sector organizations that put sound disaster recovery programs and processes in place not only gain protection, they're able to achieve competitive advantage. Entire business models are predicated on continuity of information





availability. Although much is being done in the IT and Disaster Recovery arena, it is striking how little is being done within industry to address the such issues as the loss of operating facilities, people, key skills, reputation and supply chain and telecom failure.

By leveraging the top notch talent and world-class solutions available through Nova Datacom's Information/Cyber Security (ICS), Governance, Risk and Compliance (GRC), and Enterprise Architecture (AE) Practices, as well as from our strategic Disaster Recovery Planning partners, we are confident we can help your organization define the specific strategies and tasks that must be implemented to reduce risk, satisfy compliance requirements, and achieve demanding IT disaster recovery goals and objectives.

EMERGENCY PREPAREDNESS

The only thing tougher than planning for an emergency is explaining why you didn't.

Emergencies are a part of everyday life, but the big disasters of the last 10 years have taught governments, businesses and citizens alike that there's an increasing need to prepare for emergencies.

Even though America has one of the most comprehensive and sophisticated emergency preparedness architectures in the world, this assemblage of practitioners, systems and networks

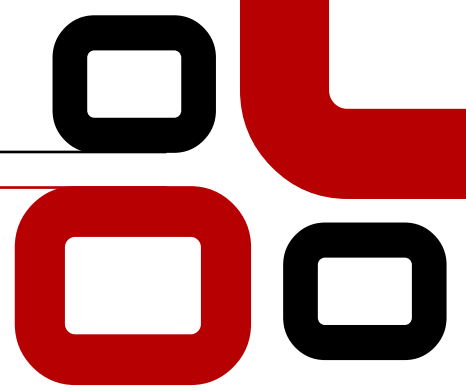


continues to evolve. It requires a continuous cycle of planning, organizing, training, equipping, exercising, and evaluation and improvement to prevent, protect against, respond to, mitigate the consequences of, and recover from a wide range of emergencies and disasters.

Members of our BCEP team have coordinated the federal response to domestic disasters, managed emergency operations centers, and have worked closely with all branches of the Federal Government (from the working level to the President's Cabinet). They have also helped state, local and foreign governments establish, maintain, test and evaluate a comprehensive array of emergency management plans, policies, procedures, teams, systems, facilities, and test, training and exercise programs.

Members of our BCEP team have worked on military operations plans, civil emergency management plans, pandemic response plans, anthrax response plans, nuclear and chemical preparedness plans and variety of special event plans—some multi-year plans, some lasting only a few days, and others being of the expedient, crisis-event driven type, such as those developed during the attacks of September 11th and continuing for weeks and months thereafter.

Our BCEP team is well-versed with the elements of world class emergency management plans, and has the operational and technical expertise to help strengthen your organization's emer-



gency preparedness posture. Our team holds industry leading patents on specific enabling technology and is known and respected for its ability to analyze and connect the dots. In addition to the traditional BCEP solutions mentioned earlier, our team also has vast experience in helping the Federal Government in the following areas:

- Anti-Terrorism/Force Protection
- Force Protection Implementation
- Security Vulnerability Assessment
- Criticality and Reliability Assessment
- Target Capabilities Assessment
- Risk and Opportunities Assessment
- CYBER/SCADA/Communications Assessment
- DCIP/FSIVA/JSIVA Assessment
- Financial System Assessment
- Disaster Assistance, Management and Recovery
- CBRNE and WMD Planning
- Logistics and Transportation
- Pandemic Vulnerability Assessment
- Pandemic Consequence Management
- Life Safety Codes Compliance
- Critical Infrastructure Protection
- Supply Chain Interdependency Vulnerability Assessment
- Training Simulation and Modeling
- Terrorism Incident Response
- Data Analysis and Acquisition
- Quality Assurance Analysis
- Capability Verification
- Building Infrastructure Standards
- Food and Water Treatment System Assessment
- Personal Identity Verification Programs

Our BCEP team can help your organization design, develop and implement a wide variety of resilience-building programs; or we can evaluate your current BCEP programs to determine the extent to they are meeting, falling below, or exceeding prescribed standards and increasingly stringent stakeholder expectations.

Our success stems from our flexibility, innovation, and deep expertise. While we have experienced exponential levels of growth, maintaining effective and nimble processes is our hallmark. We have consciously made the commitment and investment to utilize multiple technology and service vendors to provide the highest level of technical and subject matter expertise and cost-effective solutions based on client-driven requirements. We have also made heavy investments in laboratory services to ensure we can deliver the engineering mastery required in today's hyper-active BCEP environment to further support the on-time delivery of best of breed solutions and customized proof of concept demos for our clients.

We know that you share our vision of a world that is safer to live in, better prepared for the unexpected and more resilient to the threats and risks it faces. So if you need a reliable and resourceful partner to help your organization reduce risk, satisfy compliance requirements and become more resilient to an ever-increasing and dynamic set of threats and risks, call us today...you'll be glad you did.