

DISASTER RECOVERY & CONTINUITY OF OPERATIONS (COOP)

Few organizations would deny that the list of potentially business-disrupting events seems almost endless: viruses, cyber crime, power blackouts, natural disasters, and terrorist events. Even human errors and planned downtime for data migrations can create unexpected interruptions needing advanced planning. While this is easily acknowledged, unfortunately there are too many organizations that side-step the issue with continuity plans that are out-of-date, woefully inadequate, or merely unworkable.

Intekras consultants recognize the potential impact that the loss of access to governmental or commercial information or systems would have, and the cascading effect on all of the agencies and individuals who rely on that data. Our experts are well-versed in the issues associated with complying with Continuity of Operations (COOP), Continuity of Government (COG), Homeland Security Policies, and the carrying out of mission accountability at all times.

Our experts are able to assist in the mitigating of continuity risk by reviewing and recommending improvements in the following:

- Business Impact Analyses (BIA) and Risk Assessment (RA)
- Plans and Procedures
- Organizational Structure
- Human Capital
- Vital Systems, Files, Records, Databases
- Standby Facilities and Infrastructures
- Transfer of Functions/Authority
- Interoperable Communications
- Recovery and Reconstitution
- Testing & Training

“...unfortunately there are too many organizations that side-step the issue with continuity plans that are out-of-date, woefully inadequate, or merely unworkable.”

Following this analysis, *Intekras* can assist in the preparation of continuity plans. These plans will document strategies and procedures to maintain, recover, and resume critical business functions and processes and will be based on the information and priorities gathered from the BIA and RA steps. Our business continuity experts are able to draw up plans that are:

- Specific with regard to the conditions that would prompt initiation of the plan.
- Specific with regard to the immediate steps to be taken before, during, and after an incident.
- Flexible to respond to unanticipated threat scenarios and changing internal conditions.
- Focused on how to get the organization back up and running.
- Effective in minimizing service disruptions and financial loss.