

## DATA SHEET

# OPERATIONS ASSESSMENTS

Measure and Mitigate Risks

## CommsFirst Incident and Crisis Communications Services

*Prepackaged communications platforms and information tools for business continuity, public safety, and homeland security.*

### Prepare for Manmade and Natural Threats

Tornados • floods • hurricanes  
earthquakes • tsunamis • floods  
wildfires • thunderstorms  
snowstorms • power outages  
terrorists strikes • explosions  
chemical spills

### ASSESS READINESS AND MAP A PLAN

Mitigate the risks and negative impact of catastrophic events and become better equipped to protect your people, assets, and resources with CommsFirst.

For each assessment, our team of experts will:

- Identify, measure, and prioritize risks
- Determine tolerance and readiness
- Assess current standard operating procedures
- Recommend actions for mitigating risks and improving recovery
- Define processes for addressing future risks
- Document findings and action items

### ASSESSMENTS OFFERED

#### Tactical Interoperability

The ability of public agencies (police, fire, emergency medical services, and military) to communicate effectively will be studied. The assessment team will explore the capacity for sharing critical information in real time via voice, data and video, and estimate its impact on agency operations and public safety. For example, police and fire departments' capacity to coordinate efforts for managing routine activities, incidents, special events, and disasters will be evaluated.

#### Preparedness and Response

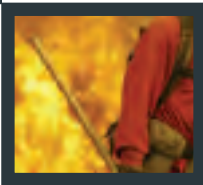
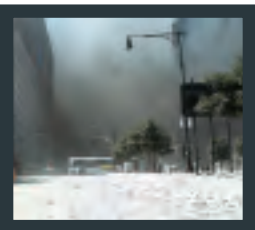
The assessment team will evaluate an organization's communications and networking, technology and data recovery, and continuity of operations in the face of a catastrophic event. In addition to technology assessments, we will evaluate the human side of communications and operations: system usability, personnel capability, individual experience in system use, and knowledge of the systems used during an incident.

#### Enterprise Risk Management

The security of an enterprise's information and telecommunications systems will be examined. Threats and vulnerabilities will be identified. The assessment team will identify internal and external threats that could result in business interruption; estimate their impact on operations, financial health, brand image, and personal safety; evaluate the enterprise's capacity to withstand downtime; and identify measures to mitigate threats to business continuity.

#### Physical Security

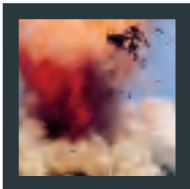
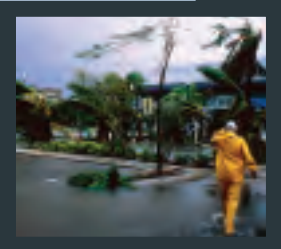
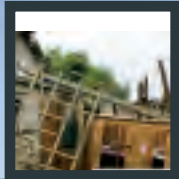
A facility's physical security and its ability to withstand natural and manmade threats will be evaluated. The assessment team will survey the facility site and building conditions, including: entries, exits, security systems, and fire alarms; shipping/receiving and loading docks; roofs and roof penetration; outside air intakes; blast resistance; building envelope protection; parking, walkways, and landscaping.



Exposure	Risks
Telecommunications	Congested and damaged networks
Electricity	Power outages
Water	Contamination
Fire	Gas line explosions
Facilities	Building damage or collapse
Security	Theft, trespassing, sabotage
Medical	Virus or pandemic
Information Technology	Hardware and software failures

### OPERATIONS ASSESSMENT METHODOLOGY | Enterprise and Public Sector

Phase	Objectives	Deliverables
<b>I. Planning</b>	<ul style="list-style-type: none"> <li>Clearly define assessment scope</li> <li>Identify and define objective, background information, roles and responsibilities</li> </ul>	<ul style="list-style-type: none"> <li>Project scope definition</li> </ul>
<b>II. Discovery</b>	<ul style="list-style-type: none"> <li>Identify and understand all risks to operations, assets, and safety</li> <li>Employ a combination of interviews, observations, audit methods, and questionnaires</li> <li>Interview key leaders to determine and establish systems criticality based upon a prioritization matrix</li> <li>Identify organizational and technical vulnerabilities</li> <li>Define recovery time objectives</li> <li>Define acceptable benchmarks</li> <li>Conduct on-site reviews at a sampling of locations as deemed necessary</li> </ul>	<ul style="list-style-type: none"> <li>Summary report of risks to critical infrastructures and current capabilities</li> <li>Hierarchical list of vulnerabilities</li> </ul>
<b>III. Asset Identification and Valuation</b>	<ul style="list-style-type: none"> <li>Identify all assets within the scope of the assessment</li> <li>Complete applications inventory, identifying key stakeholders, SOPs, location(s), dependencies, statutory and regulatory requirements</li> <li>Group and rank assets by function</li> <li>Assign asset values</li> </ul>	<ul style="list-style-type: none"> <li>Inventory listing and classification of all applicable assets and applications</li> </ul>
<b>IV. Impact Analysis</b>	<ul style="list-style-type: none"> <li>Identify and measure threats to assets</li> <li>Estimate the impact on critical operations, procedures, and personal safety</li> <li>Evaluate staffing, process controls, and technical architecture for agility and responsiveness in the context of a threat</li> <li>Assess internal compliance against stated organizational reference frameworks (i.e., ITIL, CobiT, SAS-70, PRINCE2, HIPAA, and Sarbanes-Oxley)</li> <li>Identify critical functions and facilities</li> <li>Review existing incident-response/disaster-recovery documentation and evaluate previous test scenario outcomes</li> <li>Evaluate alignment of technology plans with operational requirements</li> </ul>	<ul style="list-style-type: none"> <li>Applicable charts, tables and spreadsheets</li> <li>Threat and vulnerability analysis</li> <li>Asset/threat/vulnerability mapping</li> <li>Impact and likelihood analysis</li> <li>Risk modeling and analysis</li> <li>Downtime cost estimate report</li> <li>Risk-based SWOT and GAP analyses</li> </ul>
<b>V. Recommendations</b>	<ul style="list-style-type: none"> <li>Recommend solutions that mitigate, transfer, or eliminate the associated risk depending on the severity</li> <li>Recommend strategies for mitigating and managing future risks</li> </ul>	<ul style="list-style-type: none"> <li>An assessment report containing near- and long-term recommendations</li> <li>Prioritized recommendations listing</li> <li>Mitigation strategy report</li> </ul>
<b>VI. Conclusions</b>	<ul style="list-style-type: none"> <li>Group multiple recommendations together, analyzing the implementation strategy</li> <li>Compare different recommendations, analyzing benefits and risks of each</li> </ul>	<ul style="list-style-type: none"> <li>Final report</li> <li>Presentation</li> </ul>



Are You Ready?