Critical Infrastructure Work Group

What we do

- This Work Group started in response to calls for better IT support and coordination between emergency services first-responders (police, fire, ambulance, health, home-guard) and associated government agencies.
- The key objective is to create IT standards for shared information systems to enable coordinated decision-making on best deployment of resources.
- Longer-term objectives include assuring continuity of critical infrastructures and services.

We invite members interested in forming this Work Group to assist in defining its goals with a view to developing relevant standards and best practice guides to support delivering interoperable infrastructures.

Objectives

To identify the architectural requirements for an effective IT support system that would provide a common information systems resource across emergency services first-responders (police, fire, ambulance, health services, home-guard) plus local government and central government agencies, sufficient to be able to support the information needs of the managers of those services in the event of an emergency, so they can make best informed decisions on deployment of their combined resources in response to the emergency situation.

Further, to secure continuity of critical infrastructures and services – be they local, national, or regional – in the event of a terrorist incident or natural catastrophe.

From this shared IT information support system, develop an enterprise architecture sufficient to provide an internationally accepted foundation for effective, short-term national coordination and collaboration that secures continuity of national critical infrastructures and services.

Strategy

The strategy is to leverage current knowledge, key relationships, competent personnel, and information assets, to quickly establish an initial Critical Infrastructure Enterprise Architecture (CI-EA) framework, with sufficient coverage to include the key interests of all stakeholders, and thereby ensure they all benefit.

By leveraging the Enterprise Architecture expertise in The Open Group membership, and populating a CI-EA framework with current architectural artefacts supported by a flexible technology environment, we anticipate that a useful foundation for improved national security coordination and collaboration can be achieved quickly.

By demonstrating the benefits that deploying this CI-EA framework delivers, we anticipate it will be adopted by other authorities responsible for national security, bringing with it improved delivery of service between states, and between nations.

More Information

For more information about the Critical Infrastructure Work Group:

Email: homesec@opengroup.org

Visit: www.opengroup.org/projects/crit-infrastructure