

The Risk Analysis Workbench (RAW)
Mike Orosz, Bob Neches, and Terry Benzel
Information Sciences Institute, University of Southern California
mdorosz@isi.edu

The Risk Analysis Workbench (RAW) is a software platform in which risk-based resources (e.g., models, tools, databases, case studies, etc.) from various sources (e.g., CREATE, FAZD, START, etc.) can be accessed and shared. A long-term objective of the CREATE RAW project is to develop a common modeling environment (CME) in which various resources, with varying levels of accessibility, can be electronically “linked” to form composite analytical systems. To help achieve this goal, basic research was initiated in Year 3 in the areas of semantic networks and cyber-security technologies. In addition, a collaborative effort with FAZD Center was undertaken to develop a database server that is targeted to (in Year 4) become the infrastructure that supports server-based operations.

Over the past year, the following efforts were undertaken to improve and/or extend the CREATE Risk Analysis Workbench (RAW):

- Development of a fine-grain access control mechanism was initiated
- Enhanced software infrastructure to support future RAW server-based operations and the common modeling environment (CME)
- A new graphical user interface (based on feedback from the initial user testing), populated with new resources from the CREATE and START centers
- Extended the software to support education and outreach within the CREATE user community (support for course ISE 590 at USC).

As currently implemented, RAW is a repository of vetted resources with fine grain access control. As new “vetted” resources became available at CREATE and the other centers of excellence (COEs), they were added to RAW. The following resources were added to RAW and made available to the RAW user community over the past year:

- Models
 - NIEMO economic model (CREATE)
- Databases
 - Global Terrorism Database (START)
 - Terrorism Research Center
 - Electrical grid databases (CREATE)
- Border security case study (CREATE)
- Documentation/Reports/Links
 - Assessing and Managing the Terrorism Threat (DOJ)
 - DHS Portals
 - Risk-Based Economics Course (ISE 590) (Adam Rose course materials)

"This research was supported by the United States Department of Homeland Security through the Center for Risk and Economic Analysis of Terrorism Events (CREATE) under grant number 2007-ST-061-000001. However, any opinions, findings, and conclusions or recommendations in this document are those of the authors and do not necessarily reflect views of the United States Department of Homeland Security."

Access to a particular resource is gained by entering RAW and then downloading - to a local system (i.e., laptop, etc.) – a copy of the desired resource.

As currently implemented, RAW is a repository of vetted resources with fine grain access control. As new “vetted” resources became available at CREATE and the other centers of excellence (COEs), they are added to RAW.

Although RAW is currently a resource repository, the ultimate goal is to deliver a system that allows server-based operations, work group collaborations, and the development of composite models using resources available within RAW. In support of these objectives, the CREATE RAW team, over the past year and in collaboration with FAZD Center, began extending RAW to support server-based operations which will handle situations where it's not practical or desirable to allow users direct access to resources (i.e., the resource resides and is accessed from a RAW server). This same infrastructure will also support work group formations and the common modeling environment (CME) where various resources are electronically “linked” to form composite analytical systems.

During the Year 3 effort, a major overhaul of the cyber-security features of the system was undertaken. Previously to this effort, access control to sensitive resources was implemented with a temporary placeholder that was difficult to administer and, in some cases, open to failure. This new effort brought the RAW technology into compliance with industry specified best-practices and procedures.

In addition to improved security, a major effort, in collaboration with the FAZD Center, was initiated to enhance the RAW technology to support server-based operations. Currently, to use resources available in RAW, users must first download the selected resources to their local systems (e.g., laptop). In many cases, this may not be desirable or feasible and server-based operations will be required. It is anticipated that this capability will be available in second quarter of Year 4.

Finally, the RAW graphical user interface was greatly modified to reflect feedback from initial alpha-release testing. New graphics, messaging, and linking were implemented to help better inform the user community on topic understanding and related topics.

In the last quarter of Year 3, RAW was extended and populated with CREATE-based resources to support a risk-based economics course (ISE 590) taught by Dr. Adam Rose. Students taking Dr. Rose's course access and download course materials via the RAW graphical user interface (GUI). Dr. Garrett Asay was successfully trained by ISI on the procedures required for accessing and loading course materials into RAW. Dr. Asay then successfully trained a student to perform these same procedures.

Over the previous year, the CREATE RAW team visited all current DHS Centers of Excellence (FAZD Center, NCFPD, START, and PACER). In addition, RAW has been presented to several national labs (LLNL and PNL) and at DHS-sponsored S&T review conferences (DHS S&T Review – March 2007, NDIA HS S&T Conference – May 2007). Finally, RAW was presented to non-DHS government agencies including the NRO, DTO, and ONR. In addition, a beta version of the software was released to selected members of the DHS community outside the core RAW development environment.

Potential uses of the RAW technology in the private sector include workspace management (collaboration, resource sharing, and access control) and decision-support operations (risk assessments, current situational awareness, “what-if” analysis).