



NDCEE

National Defense Center for Energy and Environment



DoD Executive Agent

Office of the
Assistant Secretary
of the Army for
Installations, Energy and
Environment

Water Security Assessments

Elizabeth Keysar, NDCEE/CTC

18-20 January 2012

The NDCEE is operated by:  *Concurrent Technologies Corporation*

Technology Transition – Supporting DoD Readiness, Sustainability, and the Warfighter

Agenda

- Introduction to Water Security
- Water Security Assessment Purpose and Components
- Water Security Assessment Protocol
 - Baseline Data Collection and Review
 - Pre-Assessment Coordination
 - On-Site Data Collection
 - Risk and Vulnerability Analysis
 - Score Sheets and Vulnerability Self Assessment Tool
 - Risk Mitigation Prioritization

Definition of Water Security



“Army water security is the assurance that water (potable and non-potable) of suitable quality will be provided at rates sufficient to fully support the Army wherever it has, or anticipates having, a mission in the future.”

Army Security Strategy
Army Environmental Policy Institute, 2011

Water Security Assessment Purpose

To help Army Installations evaluate long-term water access, assess water system vulnerabilities, and identify security measures that should be considered to protect the system and the customers it serves.



Water Security Assessment Components

*More than traditional Vulnerability Assessment
Incorporates long-term perspective and regional factors*

Components

- Sources
- Supply
- Sustainable Practices
- Survivability
- Stakeholders
- Sponsorship

Ongoing Vulnerability Assessments

Water Security Assessment Components

WSA Components	Focus
Sources	<i>The quantity and quality of natural, raw water available to the region</i>
Supply	<i>The Army's entitlement to the raw water and means of distributing it to Army users</i>
Sustainable Practices	<i>Net Zero water use efficiency concepts</i>

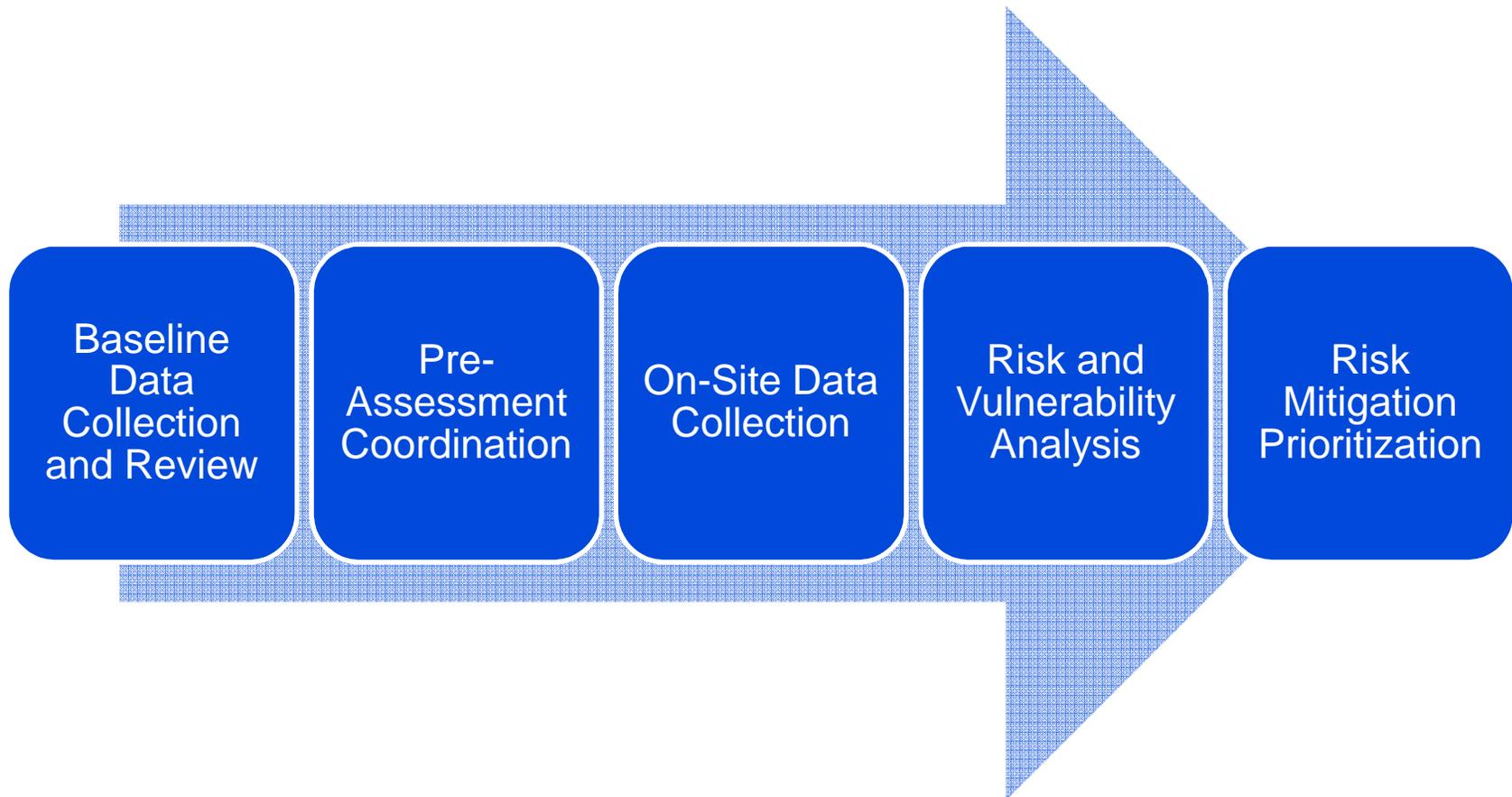
Water Security Assessment Components (Continued)

WSA Components	Focus
Survivability	<i>Preventing and recovering from water supply disruption or contamination</i>
Sponsorship	<i>Identification and alignment of water management responsibilities</i>
Stakeholders	<i>Constructive engagement of other regional water users</i>

Assessment Approach

- **Survivability**
 - United States Environmental Protection Agency (EPA) Vulnerability Self Assessment Tool (VSAT)
 - Relational database with user interface
 - Free download, easy to use; Password protected and easy to transfer dbase file
 - Non-Secret Only at first, installation can then proceed to “Secret” as needed
- **Supply, Sources, Stakeholders, Sustainable Practices, Sponsorship**
 - Interviews with installation Subject Matter Experts
 - Qualitative scoring sheets

Water Security Assessment Protocol



Risk and Vulnerability Analysis – Part 1

- Qualitative scoring process
 - Identify areas of concern related to long-term water availability and water system management.
- Not sensitive information
 - Complete and share without restrictions.
- Areas with low scores are investigated further for the identification of mitigation actions.

Water Security Assessment Score Sheets

Sponsorship Question	SCORING					
	0	1	2	3	4	5
Does the installation actively and regularly engage in local and/or regional activities directed at understanding its rights regarding water and its withdrawal, and its relationship/effect on others?	Unknown	Keeps only official materials and notifications	Read in newspapers and follows in the news – no active involvement	Keeps informed through notification and some staff follows proceedings	Some participation in activities – regularly participates in public meetings and hearings	Active participation and leadership in local and regional activities directly impacting installation's interests

Risk and Vulnerability Analysis – Part 2

- Survivability Component
 - Evaluate water system asset/threat pairs with VSAT tool
- Once critical missions and facilities are identified, prioritized and linked to threats, data can become restricted to Secret
 - Work closely with installation personnel to determine the point at which becomes Secret.

VSAT

- VSAT 5.0 provides
 - An intuitive, smart navigation controlled, step-by-step, risk assessment process
 - Embedded video tutorial guides
 - Public health and economic risk assessments
 - Countermeasure effectiveness assessments
 - Automated MS Word and MS Excel reports
 - Automated Emergency Response Plan module

VSAT Setup

VSAT 5.0 - [C:\RCA Work (CTC)\WSA\VSAT Tool\Demo1.mdb]

File View Administration Resources Help

VSAT Home Tools Setup Assets Countermeasures Threats Baseline Improvement Cost/Risk Results & Reports

Setup Summary Utility Information Water Onsite Chemicals

Utility Information

Enter your general utility information. VSAT includes applicable information in the generated analysis and reports.

Analyst/Location

Analyst Name: RCA
Phone Number: 7135035900
Fax Number:
Email Address: armstror@ctcc.com
Address: 100 CTC Drive
City: Johnstown
State: Pennsylvania ZIP: 15904
County: Cambria

Update All Assets with this Address Location

Utility Details

Utility Ownership: Public
Population Served: 25000
Utility Name: JBLM
Counties and/or Independent Cities Served:
Mission Statement:
Statement

Financial Data

Annualized Cost Calculation Method: Simple
Interest Rate on Capital Expenditures:
Years Financed:
Statement

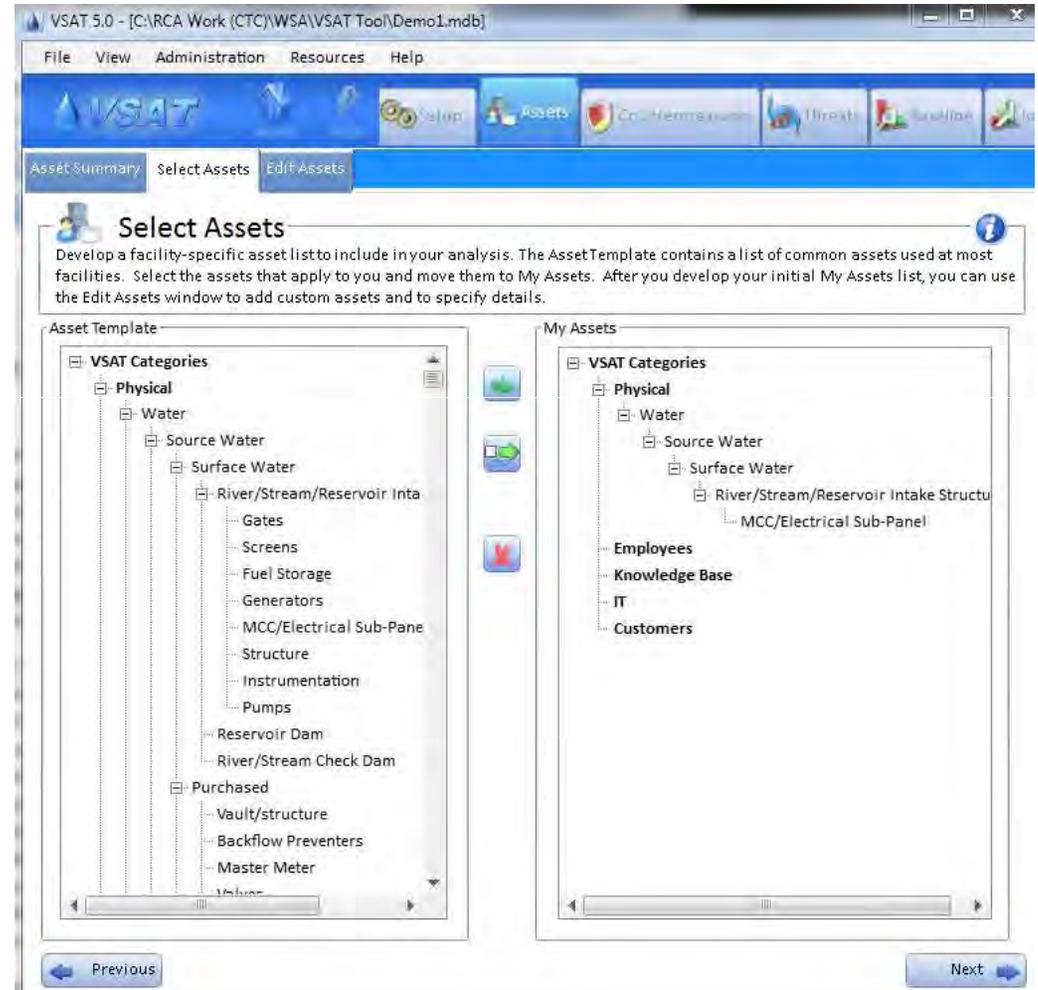
Threat Data External Links (URLS)

USGS Earthquake Hazards Program: <http://earthquake.usgs.gov/hazards/>
FEMA Flood Rate Insurance Program: <http://msc.fema.gov/webapp/wcs/stores/servlet/FemaWelcomeView?storeId=10001>

Previous Next

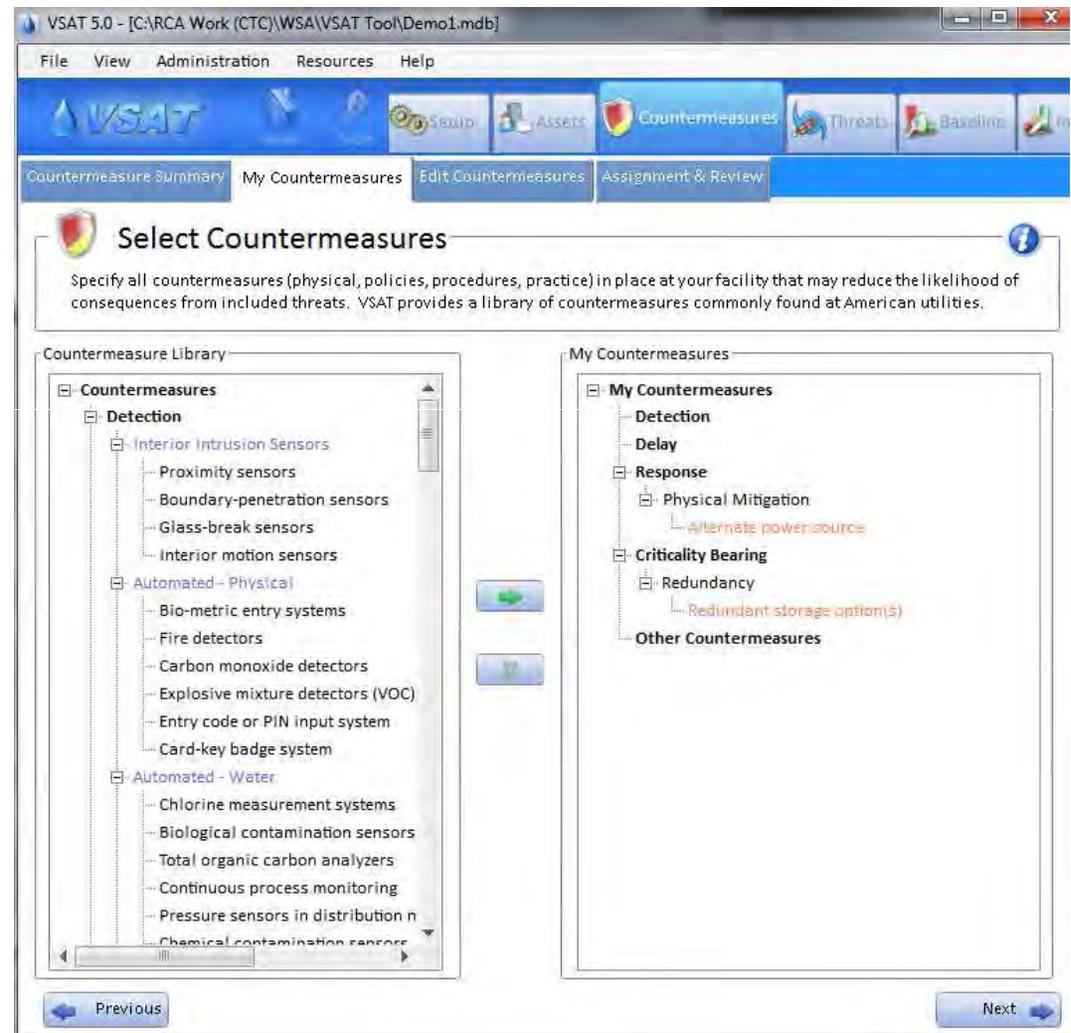
VSAT Assets

- Select and Edit Assets
 - Identify, select, update and edit specific utility assets
 - Asset Classes
 - Physical
 - Employees
 - Knowledge Base
 - Informational Technology
 - Customers



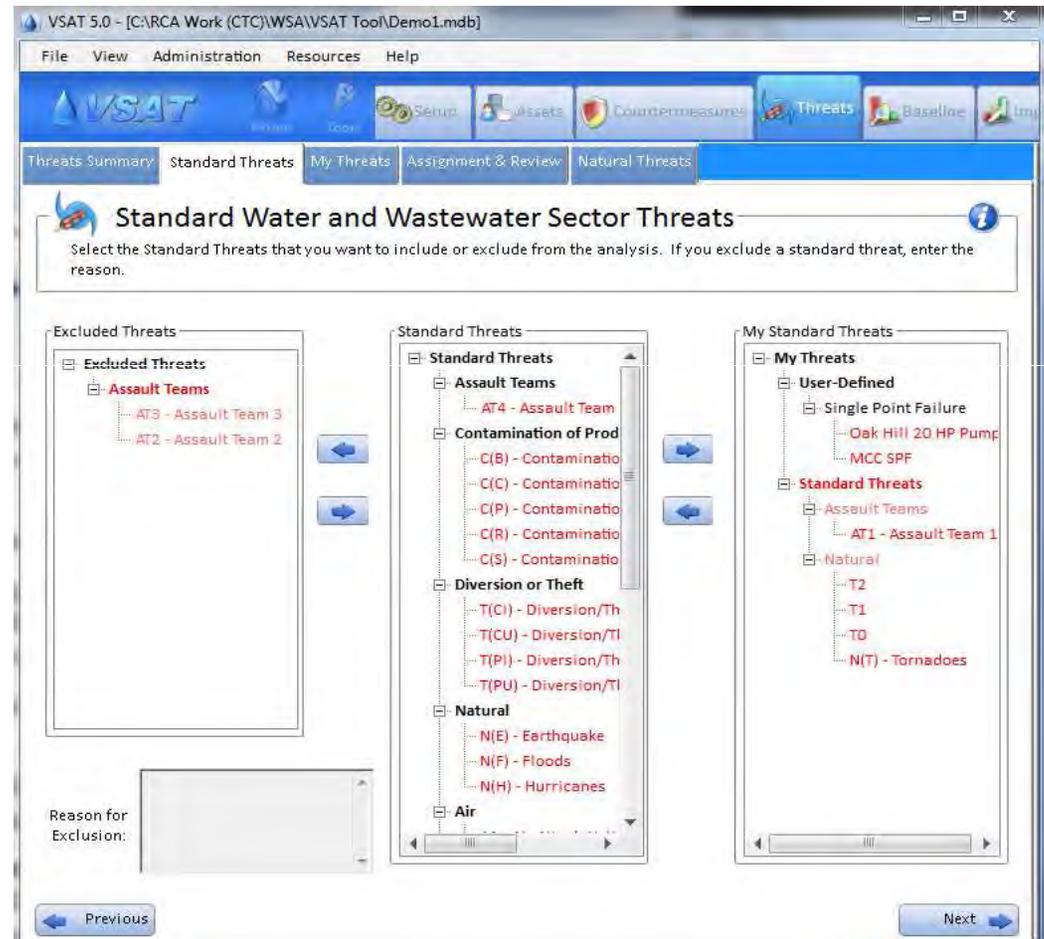
VSAT Countermeasures

- Identify then assign countermeasures per asset
- Assigned to man-made threats
 - Threat detection
 - Delay to threat detection
 - Threat response
- Natural Disasters
 - Natural disaster preparation
 - Active response
 - Recovery



VSAT Threats

- Identify existing threats and pair assets from previous developed asset list
 - Standard Threat List
 - User Developed Threat List
 - Add a “Mechanical Failure” threat for components/subsystems that do not have redundancy
 - Consider backup power as a redundancy issue



VSAT Baseline Analysis

- Identify and specify potential public health and economic consequences as well as the likelihood of those consequences and the likelihood of threat occurrence

The screenshot displays the VSAT 5.0 software interface. The title bar reads "VSAT 5.0 - [C:\RCA Work (CTC)\WSA\VSAT Tool\Demo1.mdb]". The menu bar includes "File", "View", "Administration", "Resources", and "Help". The main window is titled "Baseline Summary" and contains the following sections:

- Baseline Summary:** A text box explaining the analysis process and two approaches: "Best Estimate" (allows specific likelihood determinations) and "Conditional Risk" (assumes a 100% probability of threat occurrence).
- Select Asset/Threat:** A tree view under "Assets/Threats View" showing a hierarchy: VSAT Categories > Physical > Water > Source Water > Surface Water > River/Stream/Reservoir Intake Structure > MCC/Electrical Sub-Panel. Below this, a list of threats includes MCC SPF, N(T) - Tornadoes, T1, and T2.
- Selected Asset/Threat:** Text boxes showing "Selected Asset" as "MCC/Electrical Sub-Panel" and "Selected Threat" as "MCC SPF". A dropdown menu shows "User-Defined >> Single Point Failure".
- Asset/Threat Pairs Analyzed:** A gauge-like meter showing a value of approximately 2.5.
- Perform Baseline Analysis:** A large blue button at the bottom right.

VSAT Improvement Assessment

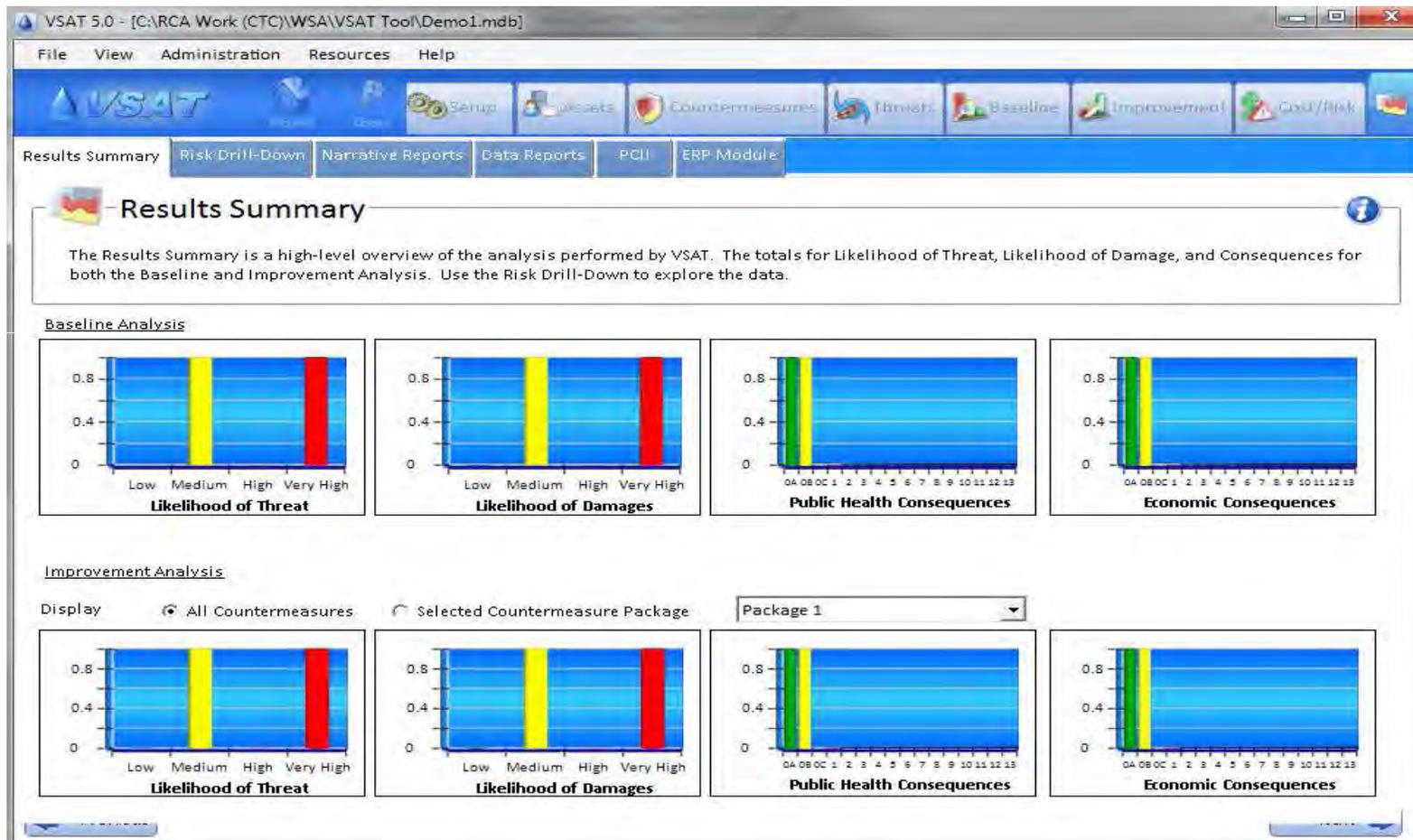
- Propose new countermeasures to reduce consequences
 - Reassess expected public health and economic consequences and re-estimate threat occurrence likelihood

The screenshot displays the VSAT 5.0 software interface. The title bar reads "VSAT 5.0 - [C:\RCA Work (CTC)\WSA\VSAT Tool\Demo1.mdb]". The menu bar includes "File", "View", "Administration", "Resources", and "Help". The ribbon contains icons for "Analysis", "Assets", "Countermeasures", "Threats", "Baseline", "Improvement", and "Consequences". The "Improvement Summary" tab is active, showing a section titled "Improvement Summary" with an information icon. Below the title, there is a paragraph: "After you customize the VSAT environment by specifying the assets you want to analyze and the threats you wish to consider, you can begin your baseline analysis. VSAT performs the analysis on one asset/threat combination at a time. VSAT supports two approaches to determine the likelihood of threat occurrence:" followed by two radio button options: "Best Estimate" and "Conditional". Below this, there are two text boxes: "Selected Asset/Threat" with "Selected Asset" set to "MCC/Electrical Sub-Panel" and "Selected Threat" set to "MCC SPF"; and "Asset/Threat Pairs Analyzed" showing two gauges labeled "Baseline" and "Improvement", both with a needle pointing to the number 2. A large blue button at the bottom right says "Perform Improvement Analysis".

VSAT Summaries and Reports

- VSAT can auto-generate:
 - Baseline Analysis Results Summary
 - Improvement Analysis Results Summary
 - Risk Drill Down Summaries
 - Asset, Threat, Countermeasure, Baseline and Improvement Analyses, and Risk Reports in MS Word
 - Baseline and Improvement Reports in MS Excel
 - Emergency Response Plan

VSAT Summaries and Reports



Risk Mitigation Prioritization

- Identify mitigation actions
 - Areas with low scores in the qualitative scoring process
 - Asset/Threat pairs highlighted in VSAT
- Installation WSA Team will need to prioritize the actions necessary to protect the system from vulnerabilities, as many of these will be in the “Secret” classification

Risk Mitigation Prioritization Factors

- Factors that can help determine priorities include:
 - Information about the likelihood of a terrorist attack or other threats
 - The primary missions supported by the system
 - Single points of failure that could severely limit capability to conduct the primary missions
 - Critical customers
 - The vulnerabilities identified by completing this assessment