

Aligned with your needs.

The Automation of a Risk Analysis and Management Methodology

Jay Robinson
Alion Science and Technology



ALION
SCIENCE AND TECHNOLOGY

www.CounterMeasures.com

www.RAMCAPPlus.com



Snapshot of Objectives

- Why automate your risk assessment/analysis program?**
- Foundational Terms and Concepts**
- Minimum Data Elements for an automated program**
- Incorporating automation into the Risk Analysis Process**



Why automate the process??

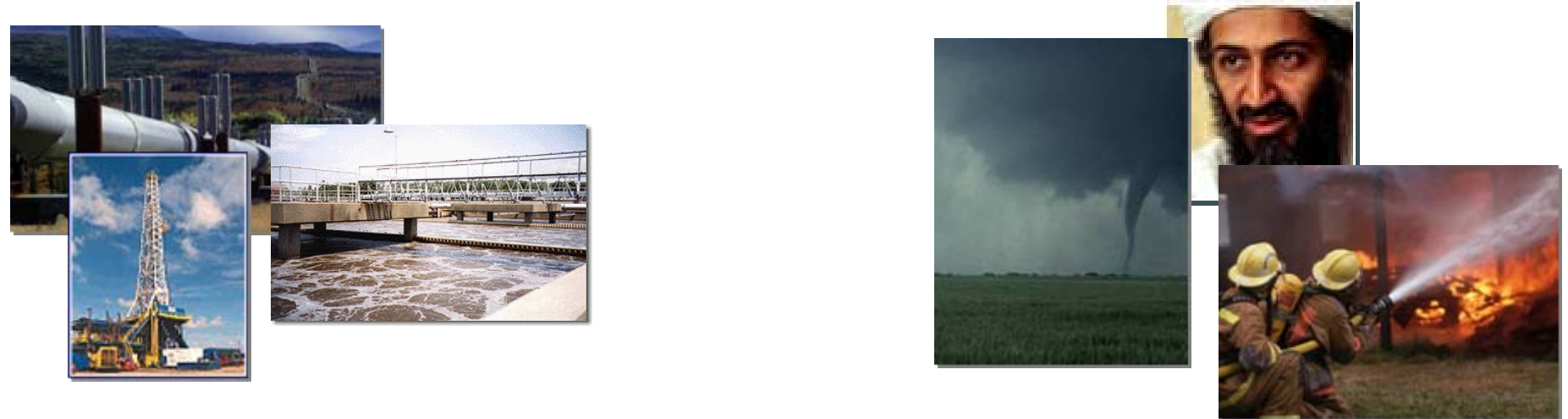
- ❑ Repeatability across large volume of assessments
 - ❑ Person-to-person
 - ❑ Place-to-place
 - ❑ Across time
- ❑ Ease of analysis
 - ❑ Data collected will always be in a standardized data format
 - ❑ Ability to analyze more data more quickly
- ❑ Communication of Risk Understanding
 - ❑ Ability to create decision support products more compelling than 3-ring binders (i.e. maps, charts, graphs, trends)
- ❑ Reusability of data
 - ❑ Reuse in other analytical tools
 - ❑ Ability to use data to satisfy a variety of reporting requirements (i.e. budgeting, inventory, plan of action, etc.)



So, how are we defining risk?

“The possibility of sustaining loss”

- ❑ *The potential for loss of, or damage to, an asset. It is measured based upon the value of the asset in relation to the threats and vulnerabilities associated with it. – FEMA 426*





How will we measure risk?

“Begin with the end in mind...”

❑ Absolute Risk

- ❑ Is the most valuable for overall enterprise risk
- ❑ Is a traditional Consequence * Threat * Vulnerability (C*V*T) calculation
 - ❑ Consequence is the asset's valuation
 - ❑ Threat includes both some measurement of severity and likelihood

❑ Single event risk (Conditional Risk)

- ❑ Is a traditional C*V*T calculation **BUT** the Threat does not have a likelihood, only a severity.
- ❑ Especially useful for rare events on which likelihood data is unavailable

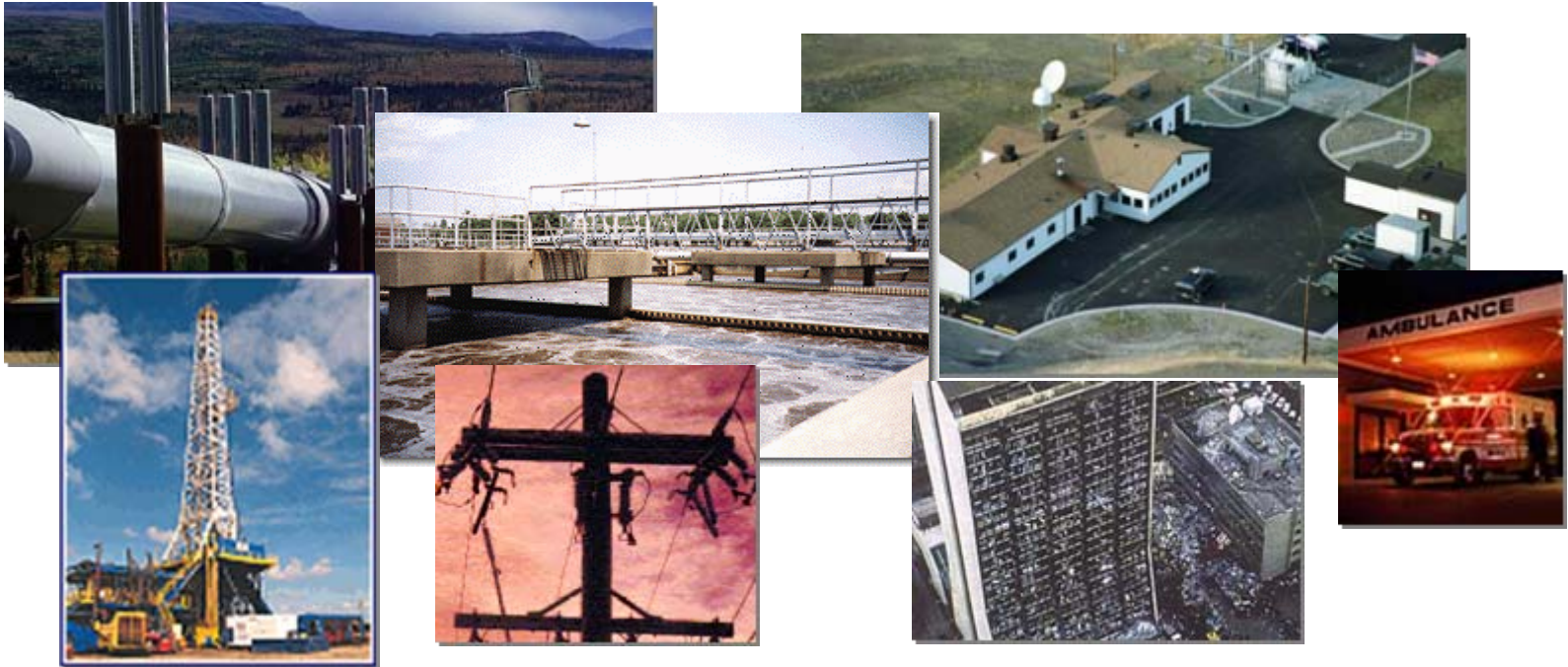
❑ Vulnerability quantification

- ❑ Is not actually a “risk” calculation, but is an important building block
- ❑ Can have stand-alone value, especially if good Consequence & Threat



Assets

Anything with value and worth protecting or preserving.





Asset Data Elements

- ❑ Mandatory to have quantification of value to the organization
 - ❑ Allows asset-to-asset comparisons
 - ❑ Does not have to be perfect, orders of magnitude is a good start
 - ❑ Can be refined over time
 - ❑ Can be based on different elements in the *same assessment* including:
 - ❑ Replacement value or Repair Costs, number of people on site
 - ❑ Business impact including loss of market share, insurance deductibles, contract fulfillment penalties
 - ❑ Mission / Business Continuity Value
 - ❑ If using a qualitative approach, each level *must* be well defined
 - ❑ Five point (VH-H-M-ML-L) is preferable to three point (H-M-L)
 - ❑ Will still have numbers behind.... Linear or non-linear
 - ❑ More than five can get clumsy
- ❑ Optional Asset Details
 - ❑ Ownership or responsibility
 - ❑ Physical location
 - ❑ License or serial numbers
 - ❑ Descriptions, etc..



Threats

Threats are events or actions with the potential to cause an impact upon assets.





Threat Minimum Details

- ❑ Severity
 - ❑ Why a Cat 5 hurricane is worse than a Cat 1.
 - ❑ Not one-dimensional; varies according to asset
 - ❑ Varies according to valuation method
- ❑ Frequency of occurrence, probability, likelihood...
 - ❑ If you want absolute risk... is required
 - ❑ Does not have to be perfect, just order of magnitude
 - ❑ Historical records
 - ❑ Empirical knowledge
- ❑ Qualitative vs. quantitative
 - ❑ Same comments as with the assets details
- ❑ Optional, but nice to have
 - ❑ Justifications, Data Sources, Documentation



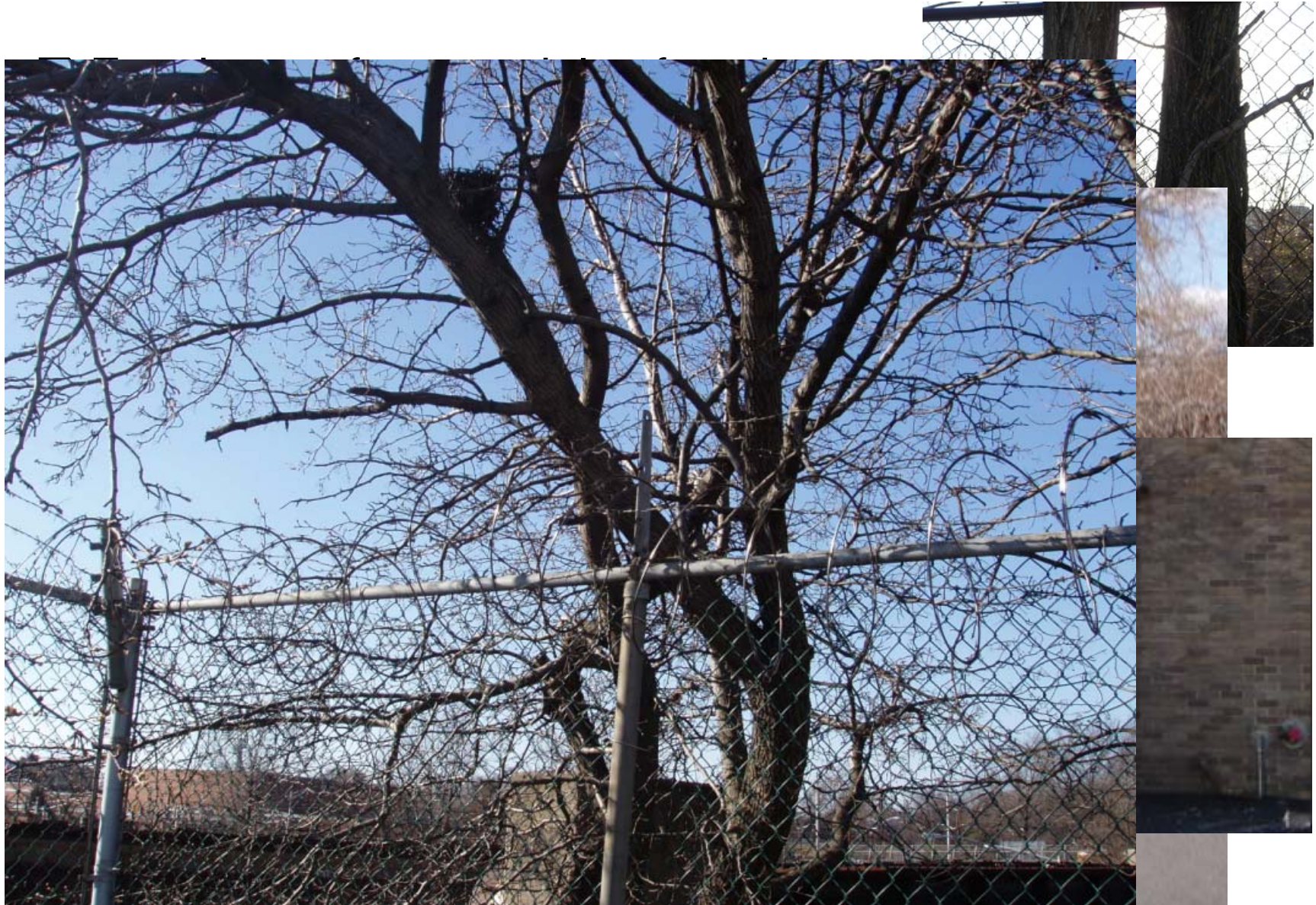
Vulnerability

Countermeasures are devices, processes, actions and/or procedures which have the susceptibility to reduce vulnerability.

- ❑ Why define Countermeasures vs. Vulnerability?
 - ❑ Countermeasures are the observable & measureable items that determine levels of vulnerability
- ❑ Vulnerability is usually not an input, but a calculation based on the presence and absence of applicable countermeasures
- ❑ Therefore:
 - ❑ Countermeasures must be weighted
 - ❑ Not one-dimensional: vulnerability specific
 - ❑ Must be in sufficient detail to allow meaningful recommendations.
 - ❑ Can be done based on compliance... but compliance does not equal risk



Based on observables!!





The Risk Analysis Process

STEP 2 Create a Plan of Action

- What guidelines, standards and regulations should be addressed?
- Data collection schedule and procedures

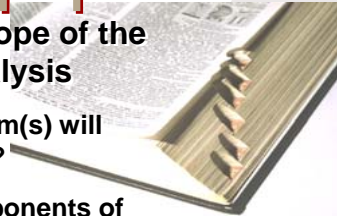


STEP 3 Configure Your Datasets

- Create checklists and surveys that cover standards, guidelines and regulations applicable for each component identified in Step 1.

STEP 1 Define the Scope of the Risk Analysis

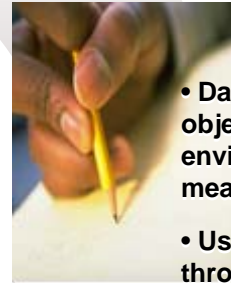
- What system(s) will be analyzed?
- What components of the system will the analysis encompass?



- Interviews?
- Surveys?
- Walk-through inspection?

STEP 4 Collect Data

- Data collection is essential to creating an objective “snapshot” of the system environment and existing system security measures.
- Using checklists during interviews and walk-throughs as well as surveys facilitates data collection.



STEP 7 Manage Risk

- Risk management includes tracking assignment and implementation of recommend countermeasures and once complete, update the analysis to reflect your new security posture.



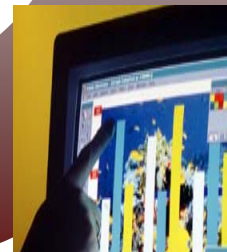
STEP 6 Create Reports

- Concise reports present management with analysis results and recommendations on how to improve security posture



STEP 5 Analyze Data

- Data is converted to meaningful numerical values that calculates vulnerability level, loss expectancy, and impact analysis. Data analysis is necessary to determine which additional countermeasures an organization should implement



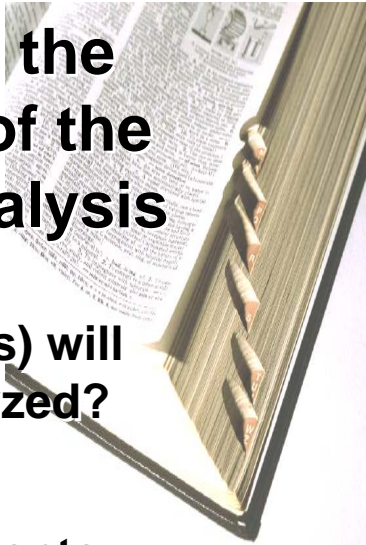


Automation Considerations in Step 1

STEP 1

Define the Scope of the Risk Analysis

- What system(s) will be analyzed?
- What components of the system will the analysis encompass?



Defining the Scope... need to know and ask

- Facility types, Systems, Networks
- Missions, Functions, Business processes
- Compliance with policies, rules, guidelines, regulations
- Each element has to have a home in the tool.
- Need to know what outputs will be desired
 - Affects free text vs. look-up fields.
 - Goes both ways. Where a tool will need

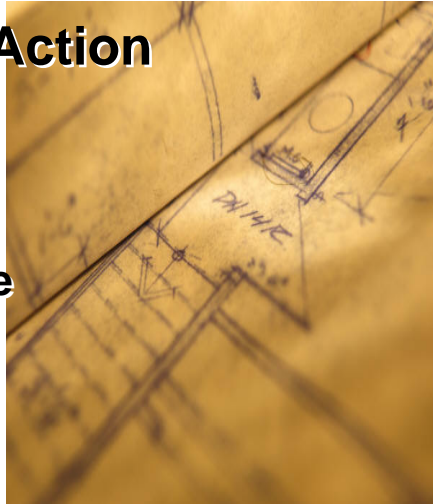


Automation Considerations in Step 2

STEP 2

Create a Plan of Action

- What guidelines, standards and regulations should be addressed?
- Data collection schedule and procedures
- Interviews?
- Surveys?
- Walk-through Inspection?



- Technology is driven by your deployment method and plan of action
 - Web based... great for rollups and updates, but needs connectivity
 - PC-Based.. Good for inspections but requires import-export and updates are problematic
 - Existing equipment? Linking?
- Content driven by staffing and time
 - Few inspectors and lots of facilities → drives level of detail



Automation Considerations in Step 3



STEP 3

Configure Your

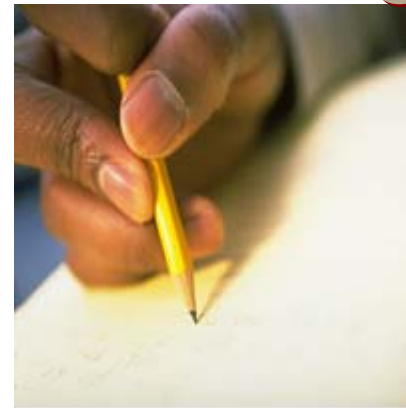
- **Create checklists and surveys that cover standards, guidelines and regulations applicable for each component identified in Step 1.**

- Done prior to conducting Surveys
 - Should include references, guidance, and how-to's...
 - Adding items on-the-fly is often requested by inspectors, but is problematic for centralized analysis
- Configuration done centrally so that standardization is assured:
 - Items are validated and weighed consistently
 - Makes sure good items are then pushed out to all users.



Automation Considerations in Step 4

- Interact with Survey Respondents
 - Inspectors?
 - Self assessments?
 - Web-based?
 - Self identified or invited
- How to collect completed surveys
- Survey process coordinated by trained analyst



STEP 4

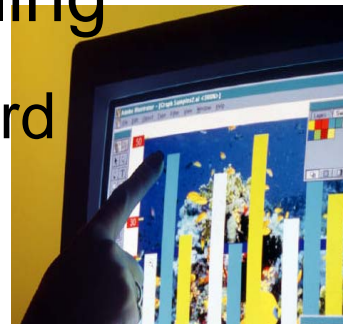
Collect Data

- Data collection is essential to creating an objective “snapshot” of the system environment and existing system security measures.
- Using checklists during interviews and walk-throughs as well as surveys facilitates data collection.



Automation Considerations in Step 5

- ❑ Initial vulnerability assessment
- ❑ “What-if” scenarios for modeling
 - ❑ Manual or using proposal wizard
- ❑ Threat/vulnerability/asset evaluations
- ❑ Compliance measurement



STEP 5 Analyze Data

- Data is converted to meaningful numerical values that calculates vulnerability level, loss expectancy, and impact analysis.
- Data analysis is necessary to determine which additional countermeasures an organization should implement



Automation Considerations in Step 6

- ❑ MS Word and Excel risk analysis reports
- ❑ Compliance measurement results
- ❑ Risk management (assignment & tracking)
- ❑ Survey information (raw data) and special test results
- ❑ Customized report generation
- ❑ REPORTS ARE NOT ALWAYS PAPER PRODUCTS
 - ❑ Exports, screens, interfaces with other programs

STEP 6 Create Reports



- Concise reports present management with analysis results and recommendations on how to improve security posture



Automation Considerations in Step 7

- Assign actions with dates
- Provide reports to management
- Track remediation activities
- Update risk assessment and compliance reports

STEP 7

Manage Risk

- Risk management includes tracking assignment and implementation of recommend countermeasures and once complete, update the analysis to reflect your new security posture.





Snapshot of Objectives

Conclusions

- Why automate your risk assessment/analysis program?**
 - Keep the End in Mind**
- Foundational Terms and Concepts**
 - Standardized terms and elements**
- Minimum Data Elements for an automated program**
 - Capturing Asset Value**
 - Capturing Threat**
 - Capturing Vulnerability**
- Incorporating automation into the Risk Analysis Process**
 - Regardless of how many steps in your process**
 - Automation needs to be considered**