



**Carnegie Mellon  
Software Engineering Institute**

Pittsburgh, PA 15213-3890

---

# **The Diagnostic Roadmap**

Progress in Developing an Integrated View of Risk  
Identification and Analysis Techniques

Ray Williams  
Kate Ambrose  
Laura Bentrem

Sponsored by the U.S. Department of Defense  
© 2004 by Carnegie Mellon University

| Report Documentation Page                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                    |                                     |                                                           | Form Approved<br>OMB No. 0704-0188                  |                                 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|-------------------------------------|-----------------------------------------------------------|-----------------------------------------------------|---------------------------------|
| Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. |                                    |                                     |                                                           |                                                     |                                 |
| 1. REPORT DATE<br><b>2004</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                    | 2. REPORT TYPE                      |                                                           | 3. DATES COVERED<br><b>00-00-2004 to 00-00-2004</b> |                                 |
| 4. TITLE AND SUBTITLE<br><b>The Diagnostic Roadmap: Progress in Developing an Integrated View of Risk Identification and Analysis Techniques</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                    |                                     |                                                           | 5a. CONTRACT NUMBER                                 |                                 |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                    |                                     |                                                           | 5b. GRANT NUMBER                                    |                                 |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                    |                                     |                                                           | 5c. PROGRAM ELEMENT NUMBER                          |                                 |
| 6. AUTHOR(S)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                    |                                     |                                                           | 5d. PROJECT NUMBER                                  |                                 |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                    |                                     |                                                           | 5e. TASK NUMBER                                     |                                 |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                    |                                     |                                                           | 5f. WORK UNIT NUMBER                                |                                 |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)<br><b>Carnegie Mellon, Software Engineering Institute, 4500 Fifth Avenue, Pittsburgh, PA, 15213-2612</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                    |                                     |                                                           | 8. PERFORMING ORGANIZATION REPORT NUMBER            |                                 |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                    |                                     |                                                           | 10. SPONSOR/MONITOR'S ACRONYM(S)                    |                                 |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                    |                                     |                                                           | 11. SPONSOR/MONITOR'S REPORT NUMBER(S)              |                                 |
| 12. DISTRIBUTION/AVAILABILITY STATEMENT<br><b>Approved for public release; distribution unlimited</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                    |                                     |                                                           |                                                     |                                 |
| 13. SUPPLEMENTARY NOTES                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                    |                                     |                                                           |                                                     |                                 |
| 14. ABSTRACT                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                    |                                     |                                                           |                                                     |                                 |
| 15. SUBJECT TERMS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                    |                                     |                                                           |                                                     |                                 |
| 16. SECURITY CLASSIFICATION OF:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                    |                                     | 17. LIMITATION OF ABSTRACT<br><b>Same as Report (SAR)</b> | 18. NUMBER OF PAGES<br><b>21</b>                    | 19a. NAME OF RESPONSIBLE PERSON |
| a. REPORT<br><b>unclassified</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | b. ABSTRACT<br><b>unclassified</b> | c. THIS PAGE<br><b>unclassified</b> |                                                           |                                                     |                                 |



## *The Scene*

You're in an alternate universe...

You may be sick...

No hospitals...no general practitioners...no AMA...

“Doctors” are self-declared...

But there *are* lots of people who have designed and built blood labs...MRIs...EKGs...

*And they all want you to use  
their diagnostic tool!*



## **You're Living There Now...**

There are no “general practitioners” to go to...

There is no “AMA” of consultants to acquisition programs...

There are many choices of risk-based diagnostics:





# ***We have to do better than this!***

## **We need general practitioners to**

- **help acquisition programs understand when their symptoms are not “normal”**
- **recommend appropriate diagnostics**
- **guide programs to appropriate interventions or toward “healthy lifestyles”**

## **These GPs need**

- **knowledge of various diagnostics—pros & cons**
- **guidance in choosing any particular diagnostic or sequence of diagnostics**
- **a “patient file,” kept over time, that includes the diagnostic results**



# **The SEI Chief Engineer**

The SEI has four: Army, Navy, Air Force, Civil/Intel

They each have

- **Education, experience, knowledge and expertise in a broad range of technologies, disciplines, areas**
- **In-depth knowledge in particular areas, but not in all areas**
- **Interest in the overall health of all programs in their “practice” —unbiased, detached, impartial**

***They are ideally placed to become the “general practitioners” we need—they just need more complete “reference materials”***

***Other organizations can take on a similar role as well, but everyone needs a “roadmap”***



# Diagnostics—Two Kinds

## Model Based:

Focused on how things should be and how much you deviate from that model—should create *findings*

## Risk Based:

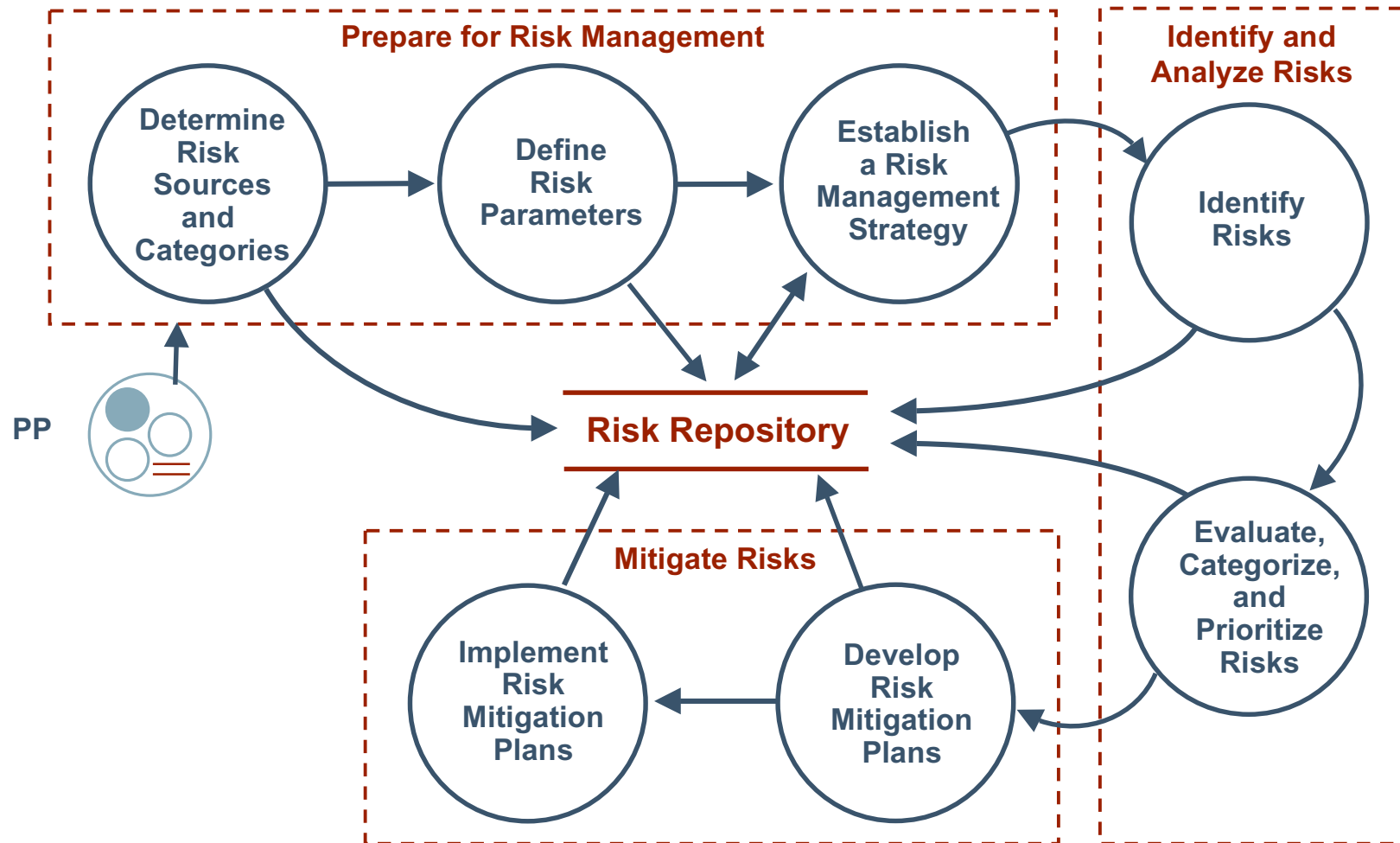
Focused on what you are doing and what risks you run in continuing—should create *risk items*

***We have chosen to only look at risk-based diagnostics in this initial roadmap work.***

***Model-based diagnostic can be added later.***

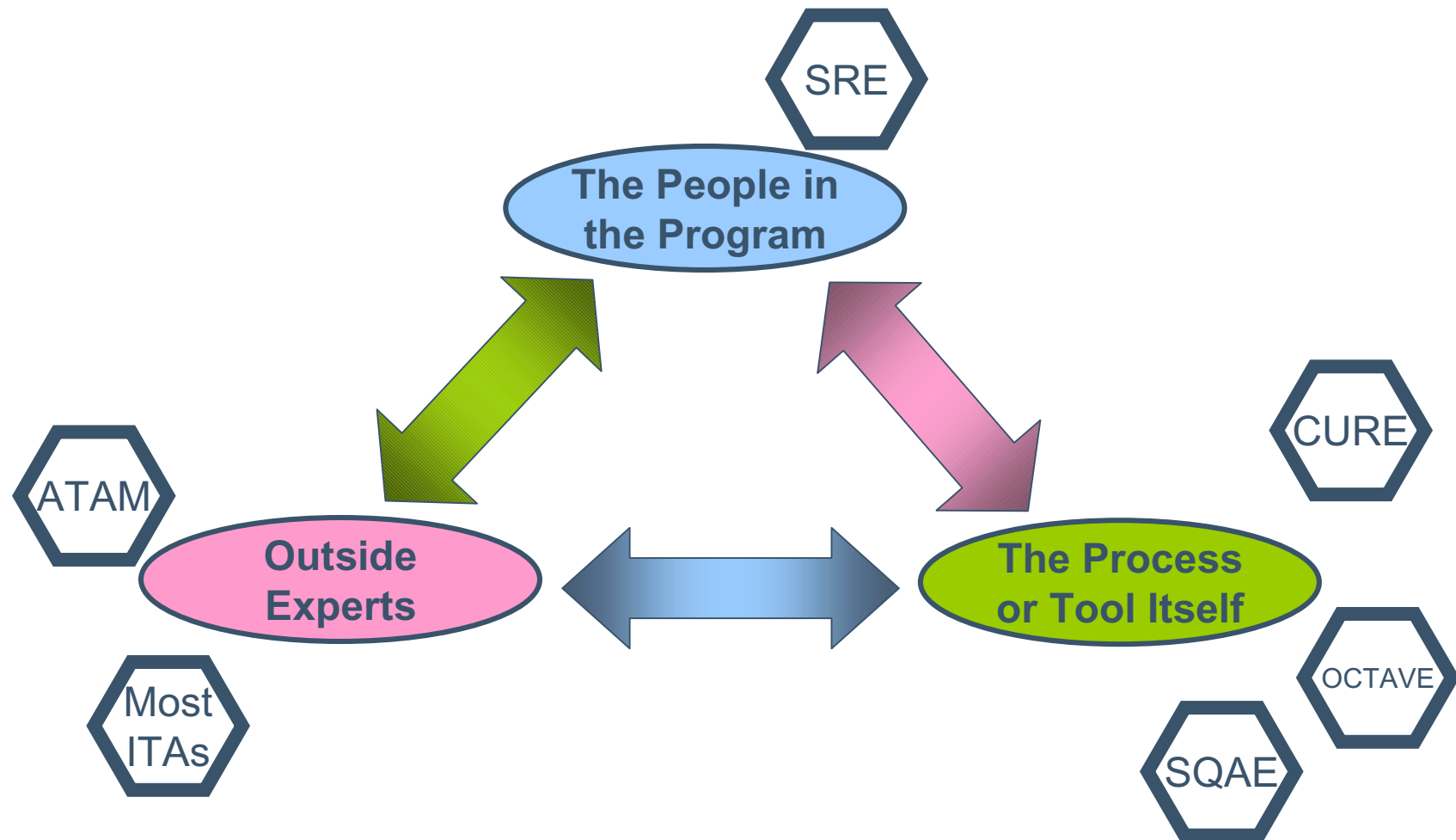


# Context for Risk Items—CMMI®





# Primary Sources of Risk Items





## **How did we identify the initial diagnostic methods that should be included in the roadmap?**

We started with the ones we knew.

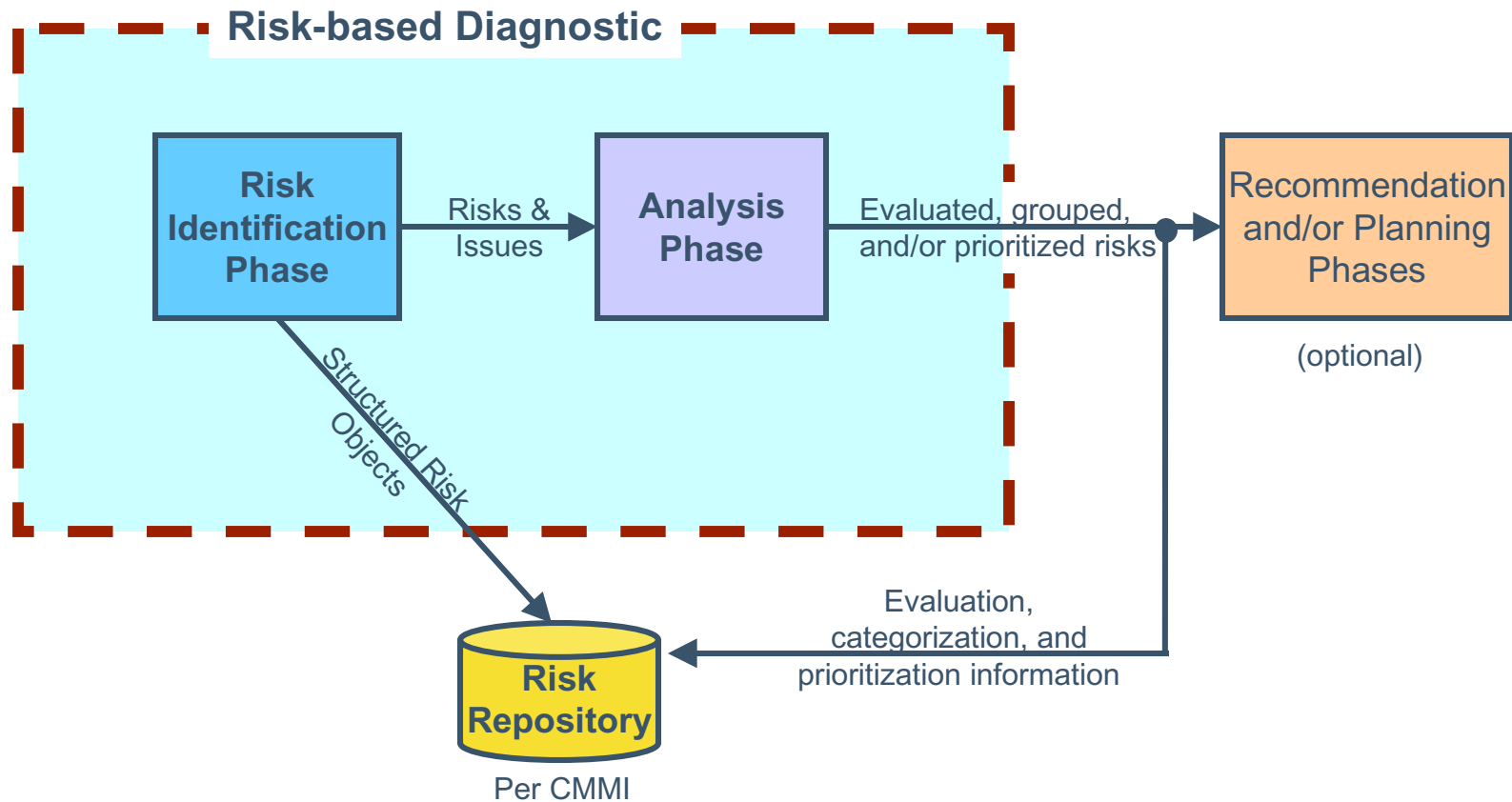
If we could explain what characteristics qualified them to be on the list, we could then go out and find others like them.

These emerged as the key qualifiers:

- Risk identification phase
- Analysis phase
- Potential risk statement “leave behind”



# Risk-Based Diagnostics





## First Three Diagnostic Methods

SRE: *Software Risk Evaluation*—facilitation-based process to document and analyze all risks already known by people in a project

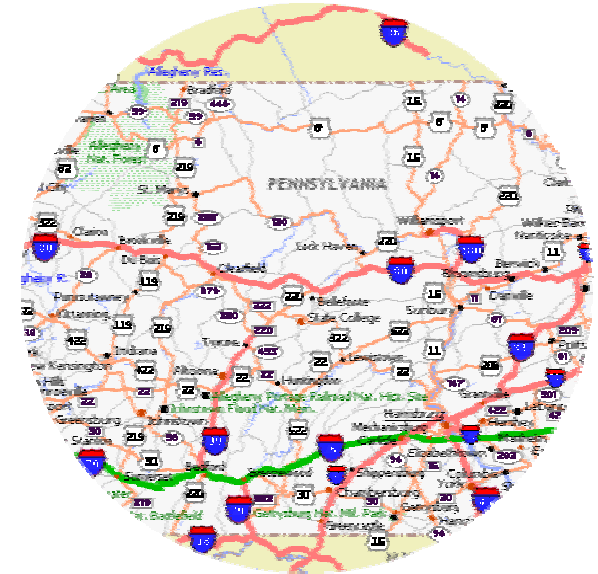
ATAM: *Architecture Tradeoff Analysis Method*—scenario-driven process to analyze a proposed or existing system architecture for inherent risks

CURE: *COTS Usage Risk Evaluation*—rules-driven process to identify and analyze the risks in a project's application of COTS products



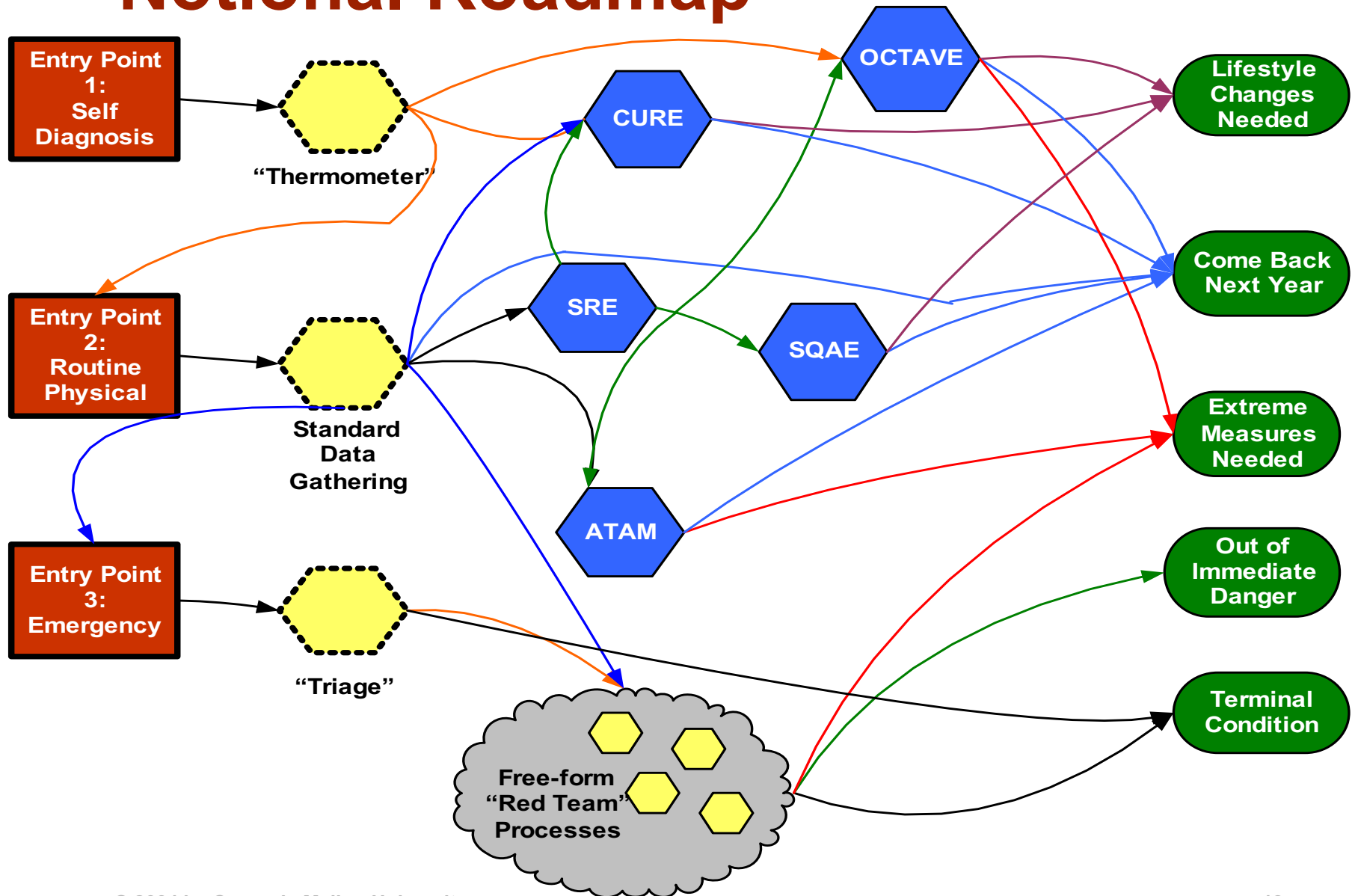
## Creating the Roadmap

- Follow the medical analogy
- Begin the “roadmap” for risk-based diagnostics with at least 3 entry points:
  - “Thermometer” (self diagnosis)
  - “Routine Physical”
  - “Emergency”
- Define a reasonable number of exit points (5 so far)
- Plug in the diagnostics we know and understand today in some reasonable sequence
- Find other risk-based diagnostics that meet our definition and plug them in
- Identify missing discriminators and currently undefined diagnostics



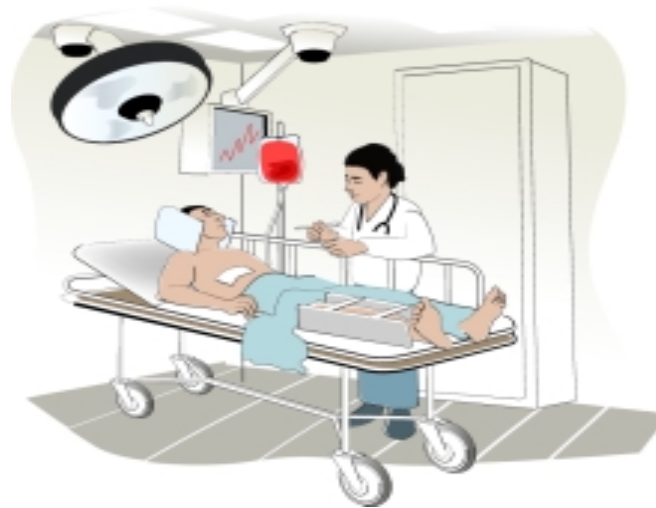


# Notional Roadmap





# Entry Points





# **Entry Point 1—“Thermometer”**

**Program recognizes symptoms of potential problems**

**Program administers self-diagnostic tool—no expert needed**

**Tool provides a reading**

- **Easy to interpret**
- **Single “snapshot” measurement**
- **Based on generally accepted picture of health**

**May seek help depending on reading (temperature)**

**If results are sufficiently alarming, will go to their own GP or seek one out**



## **Entry Point 2—Checkup/Physical**

**Program (“patient”) not necessarily feeling “sick”**

**Program enlists the assistance of GP to maintain good program health; may or may not have a prior relationship with the GP**

**GP uses interview and simple risk-based diagnostics (TBD—may be surveys, checklists), and may prescribe more costly risk-based diagnostics**

**GP reviews diagnostic results and decides whether to recommend aggressive “treatment”**

**GP may opt for emergency treatment at any time**



## **Entry Point 3—Emergency**

**Program (“patient”) knows something is wrong and requires immediate attention (critical care)**

**Program calls in the GP for intervention (“emergency rooms” don’t exist yet)**

**GP recommends course of action to address immediate problem**

**“Patient records” are updated**

**Further assessment needed to determine long-term health plan**



# Exit Points

## **Come Back Next Year**

No further diagnostics needed; keep on doing what you're doing

## **Lifestyle Changes Needed**

No immediate danger, but you're headed for trouble

## **Extreme Measures Needed**

You can be saved, but we have to act fast

## **Out of Immediate Danger**

We've saved you for now; go back to your GP's care

## **Terminal Condition**

Recovery is not possible; cut losses and terminate

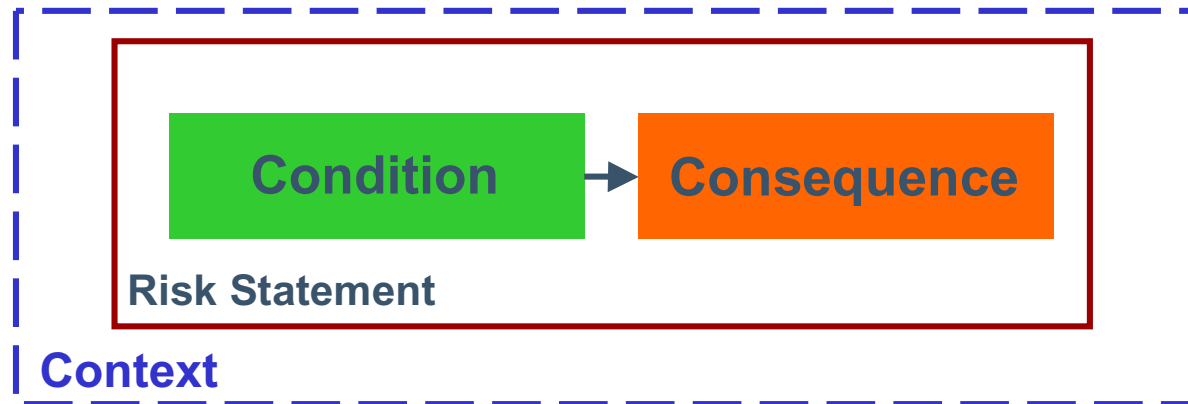


# The Risk Item

So far, only the SRE defines the structure of the risk item, so it becomes our interim model

The SRE risk item (“Risk Statement”):

- a factual **condition** statement, followed by
- at least one possible **consequence** of that condition
- supplemented with **context** for complete understanding.



*“There is water on the hall floor; someone could slip and fall.”*



## What's next

Collaborate with others to identify additional methods to be included in the Roadmap; first candidates:

- Software Quality Assessment Exercise (SQAЕ – developed by MITRE)
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE®)

Cast our net wider: solicit risk based diagnostics from all other sources

Put Roadmap in the hands of Chief Engineers and other agencies consulting to government acquisition programs for validation



# Schedule and Deliverables

