

Security Risk Management: Common Lexicon Project



Internet: www.sarma.org

Phone: (703) 635-7906

Fax: (703) 635-7935

Agenda



- The Lexicon Problem
- The SARMA Solution
- Key Success Factors
- Methodology

The Problem

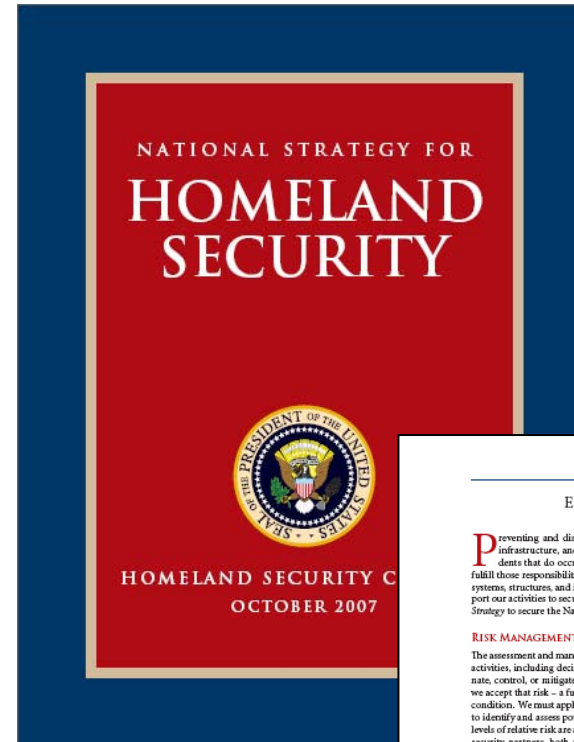
- Methodology and terminology have grown and incubated in a number of government agencies, companies, and academic circles **without sufficient overlap**, resulting in confusion, misunderstanding, and incompatibility of results.
- Progress in security risk analysis is hampered by the inability of practitioners to communicate with each other about progress and needed improvements.
- The continued development of government methodologies absent the resolution of this problem resembles the building of biblical Tower of Babel.
- The problem has eluded a government-led solution for nearly two decades.



The Problem

“A disciplined approach to managing risk will help to achieve overall effectiveness and efficiency in securing the Homeland. In order to develop this discipline, we as a Nation must organize and help **mature the profession** of risk management by adopting common risk analysis principles and standards, as well as a **professional lexicon.**”

- Nat'l Strategy for Homeland Security, 2007



ENSURING LONG-TERM SUCCESS

Preventing and disrupting terrorist attacks; protecting the American people, critical infrastructure, and key resources; and responding to and recovering from those incidents that do occur are enduring homeland security responsibilities. In order to help fulfill those responsibilities over the long term, we will continue to strengthen the principles, systems, structures, and institutions that cut across the homeland security enterprise and support our activities to secure the Homeland. Ultimately, this will help ensure the success of our Strategy to secure the Nation.

RISK MANAGEMENT

The assessment and management of risk underlies the full spectrum of our homeland security activities, including decisions about when, where, and how to invest in resources that eliminate, control, or mitigate risks. In the face of multiple and diverse catastrophic possibilities, we accept that risk – a function of threats, vulnerabilities, and consequences – is a permanent condition. We must apply a risk-based framework across all homeland security efforts in order to identify and assess potential hazards (including their downstream effects), determine what levels of relative risk are acceptable, and prioritize and allocate resources among all homeland security partners, both public and private, to prevent, protect against, and respond to and recover from all manner of incidents. A disciplined approach to managing risk will help to achieve overall effectiveness and efficiency in securing the Homeland. In order to develop this discipline, we as a Nation must organize and help mature the profession of risk management by adopting common risk analysis principles and standards, as well as a professional lexicon.

CULTURE OF PREPAREDNESS

Our entire Nation shares common responsibilities in homeland security. In order to help prepare the Nation to carry out these responsibilities, we will continue to foster a Culture of Preparedness that permeates all levels of our society – from individual citizens, businesses, and non-profit organizations to Federal, State, local, and Tribal government officials and authorities. This Culture rests on four principles.

The first principle of our Culture of Preparedness is a shared acknowledgment that creating a prepared Nation will be an enduring challenge. As individual citizens we must guard against complacency, and as a society we must balance the sense of optimism that is fundamental to the American character with a sober recognition that future catastrophes will occur. The certainty of future calamities should inform and motivate our preparedness, and we will continue to emphasize the responsibility of the entire Nation to be flexible and ready to cope with a broad range of challenges.

The second principle is the importance of individual and collective initiative to counter fundamental biases toward reactive responses and approaches. Our Culture, therefore, must encourage and reward innovation and new ways of thinking as well as better align authority and responsibility so that those who are responsible for a mission or task have the authority to act.

Failure Factors



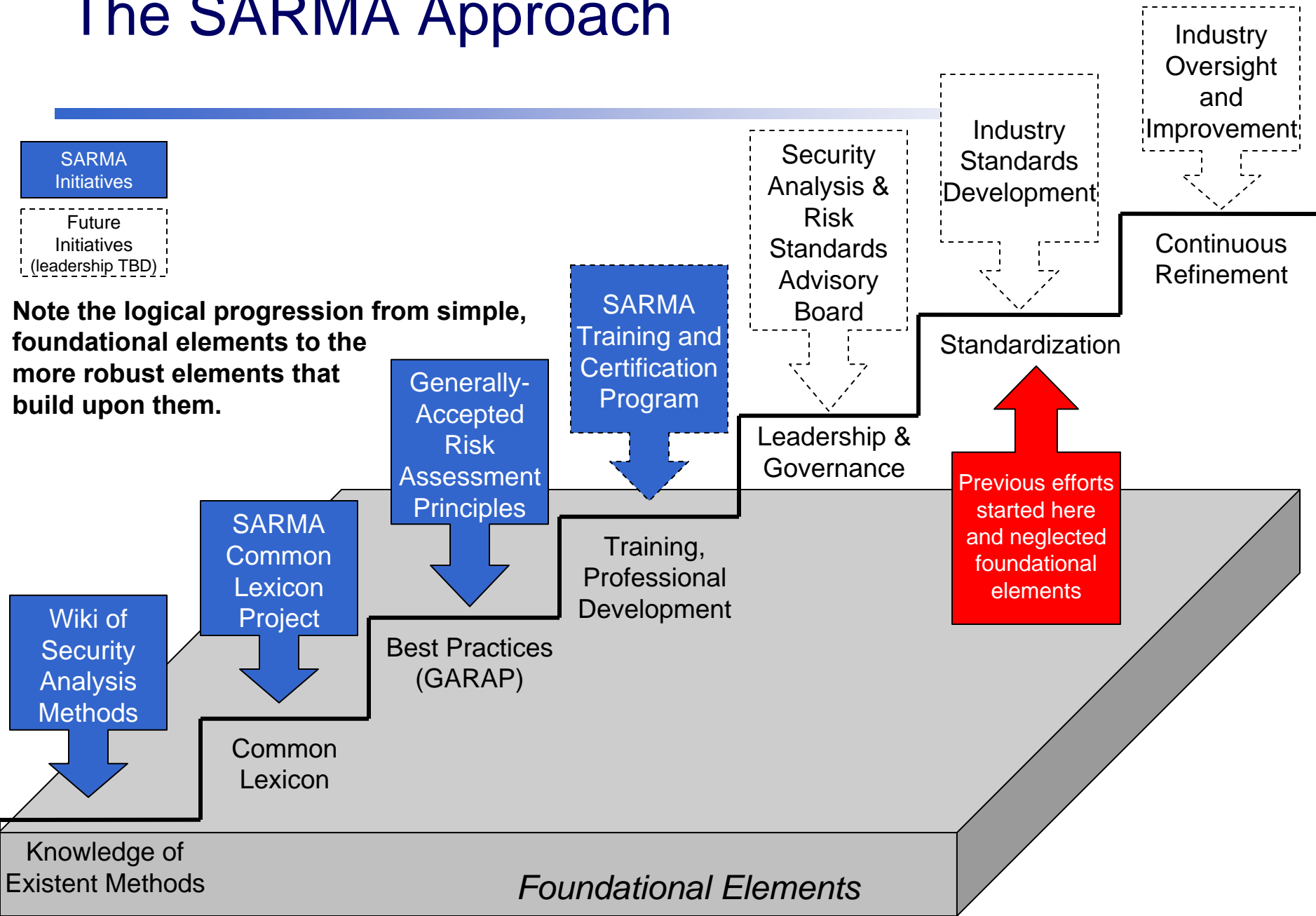
- Past attempts to standardize common lexicon in security analysis have all failed because:
 - The lack of opportunity for industry participation ensured lack of consensus and buy-in
 - Their champions attempted mandated standards but lacked organizational authority to dictate standards to others
 - Their standard lexicons failed to meet the needs of users outside of their own sphere of awareness
 - Their standards were often thinly-veiled attempts at promoting a commercial solution

Standards



- **Company and Government standards**
 - Company standards are dictated within an individual corporation, and government standards are dictated within the government. Both of these are standards governing internal practices of those limited bodies.
- **Industry standards**
 - are agreed upon by all the major actors in a given industry, but without the reasonable input of third parties, consumers, or other concerned entities.
- **Legal standards**
 - are instituted by law and international standards instituted by treaty, both of which are widely accepted but rigid and unresponsive.
- **Voluntary consensus standards**
 - specifically require that due-process procedures be created to ensure the concerns of all parties are accounted for fairly.
 - includes widespread participation such that all interested parties are accounted for, with an open forum for unfettered debate and protections for minority viewpoints
 - ensure a consensus, rather than majority, decision-making system.

The SARMA Approach



Essential Success Elements

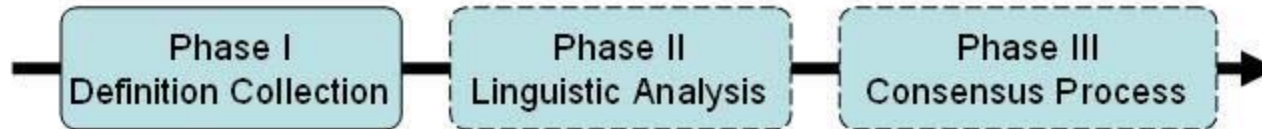


1. **Voluntary Consensus** (as opposed to dictated standards)
 - Openness
 - Balance of Interest
 - Due Process
 - An Appeal Process

2. **Inclusive Development**
 - Across federal agencies, S&L governments, and the private sector

3. **Technology Facilitated**
 - SARMA-Wiki Collection and Collaboration Tools
 - Concept Mapping and Linguistic Deconstruction (Perigean Technologies)

Methodology Overview



- **Phase I Definition Collection**
 - Begins with collection of currently-used definitions provided by anyone on the SARMApedia wiki
- **Phase II: Concept mapping redacts all definitions to core terms:**
 - Allows discussion distinct from parochial and unique interests
 - Separates core ideas from secondary ideas and gratuitous verbiage
- **Phase III: Discussion amongst a team of experts creates a proposed definition**
 - Concept mapping process shows clear origins and thought process

Methodology – Phase I

- Wiki Functionality aids documentation effort
 - **Article** provides current state of knowledge
 - **Discussion** allows practitioner debate even after initial consensus and publication
 - All users can **edit** in Phase I
 - **History** documents all changes, sourcing to user and remaining available in a perpetual archive



The screenshot shows a Wiki page for the term "Asset". At the top, there are four tabs: "article" (highlighted in yellow), "discussion", "edit", and "history". Below the tabs, the word "Asset" is displayed in a large font. A red rectangular box highlights the word "Asset" in the main content area. In the top left corner, there is a blue arrow pointing towards the "article" tab. On the left side, there is a sidebar with the SARMA logo and the text "Security Analysis and Risk Management Association". Below the logo, it says "common knowledge base" and lists "SARMApedia Home" and "Definitions". At the bottom of the page, there is a "Contents [hide]" button.

Methodology – Phase I



Asset

(Difference between revisions)

Revision as of 21:07, 20 July 2007 (edit)

Hartera (Talk | contribs)

← Previous diff

Line 32:

```
[ASME-ITI|Risk Analysis and Management for Critical Asset Protection (RAMCAP)]<ref>
[http://www.asme-iti.org/RAMCAP/Terminology.cfm RAMCAP and Risk Terminology]
</ref> |=
```

```
[5]Contracts, facilities, property, electronic and non-electronic records and documents,
unobligated or unexpended balances of appropriations, and other funds or resources
(other than personnel).[DHS|National Infrastructure Protection Plan (NIPP)
|<ref>National Infrastructure Protection Plan (NIPP), 2006
[http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf]</ref> |=
```

```
}}
```

Revision as of 14:44, 21 July 2007 (edit) (undo)

Hartera (Talk | contribs)

Next diff →

Line 32:

```
[ASME-ITI|Risk Analysis and Management for Critical Asset Protection (RAMCAP)]<ref>
[http://www.asme-iti.org/RAMCAP/Terminology.cfm RAMCAP and Risk Terminology]
</ref> |=
```

```
[5]Contracts, facilities, property, electronic and non-electronic records and documents,
unobligated or unexpended balances of appropriations, and other funds or resources
(other than personnel).[DHS|National Infrastructure Protection Plan (NIPP)
|<ref>National Infrastructure Protection Plan (NIPP), 2006
[http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf]</ref> |=
```

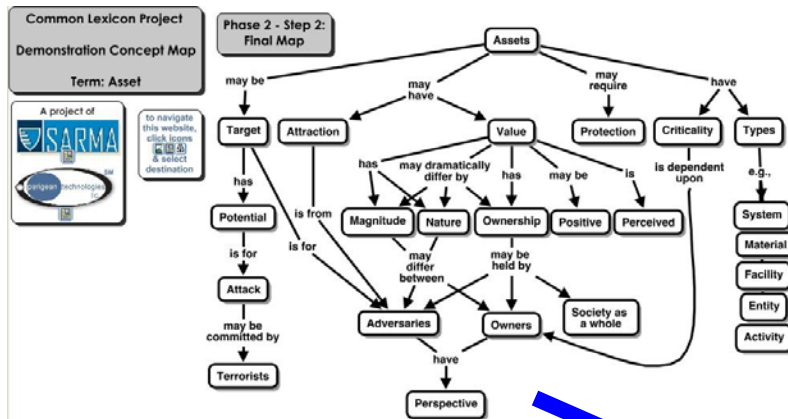
```
+ [1]A distinguishable network entity that provides a service or capability. Assets are
+ people, physical entities, or information located either within or outside the United
+ States and owned or operated by domestic, foreign, public, or private sector
+ organizations.
```

```
[DOD |Defense Critical Infrastructure Program (DCIP) Guidelines |<ref>
+ [http://www.dtic.mil/whs/directives/corres/pdf/302040p.pdf Department of Defense
+ Directive No. 3C20.40, dated August 19, 2005]</ref> |=
```

```
}}
```

In the screenshot above, you can see an example of the revision tracking inherent in the MediaWiki technology. Every revision ever made to a page is tracked, word by word and line by line, and tagged with the date, time, and user ID of the editor. In this example, the sixth definition of Asset was added to SARMA Wiki based on information from a DoD directive on DCIP.

Methodology – Phase II



Discussion by panel of experts results in dictionary and encyclopedia entry for each term – this explanation makes the process explicable and transparent to later readers.

SARMA Consensus Definition

An asset is something of value that may be subject to harm or hazard.

Definition Context

Several key issues arose during the discussion of the asset concept map while generating an agreed core definition.

1) Targeting: Almost all definitions of asset currently include explicitly or implicitly the concept that assets are targeted by ...

Methodology – Phase I

- Collect Current Definitions

Common Definitions

CIA Definitions

Private Industry Definitions

DHS / NIPP Definitions

DOD Definitions

DEF ID	DEFINITION	ORGANIZATION	METHODOLOGY NAME	REFERENCE (?)
1	In business and accounting an asset is any economic resource controlled by an entity as a result of past transactions or events and from which future economic benefits may be obtained. Examples include cash, equipment, buildings, and land.	Common	Wikipedia	[1]
2	Any person, facility, material, information, or activity which has positive value and requires protection. The asset may also have value to an adversary, although the nature and magnitude of the values may differ.	CIA	Analytical Risk Management (ARM)	[2]
3	Any person, facility, material, information, or activity that has positive value to its owner. The asset may also have a given level of value to an adversary, as well as its owner, although the nature and magnitude of the values may differ dramatically.	Independent	Analytical Risk Management (ARM)	[3]
4	Any people, facility, physical system, cyber system, material, information, activity or intangible attribute that has positive value to an owner or to society as a whole and requires protection. General organizational context: An asset whose absence or unavailability would significantly degrade the ability of an organization to carry out its mission. Functional context for asset owner: An asset whose absence or unavailability would represent an unacceptable business consequence, i.e., for which the sum of the consequences of its loss represents an unacceptable financial or political impact on the owner. <ul style="list-style-type: none"> ■ Attractive Asset – An asset that, in the perspective of the adversary, appears to be a desirable target. The nature and magnitude of the value of an asset, i.e., what makes it attractive to an adversary, may differ from the value perceived by the owner. ■ Critical Asset – The criticality of an asset varies depending on the perspective of the analyst. The following relative definitions are suggested:(sic) 	ASME-ITI	Risk Analysis and Management for Critical Asset Protection (RAMCAP)	[4]
5	Contracts, facilities, property, electronic and non-electronic records and documents, unobligated or unexpended balances of appropriations, and other funds or resources (other than personnel).	DHS	National Infrastructure Protection Plan (NIPP)	[5]
6	A distinguishable network entity that provides a service or capability. Assets are people, physical entities, or information located either within or outside the United States and owned or operated by domestic, foreign, public, or private sector organizations.	DOD	Defense Critical Infrastructure Program (DCIP) Guidelines	[6]
7	Any potential target of terrorist attack, most commonly people, equipment, a building, or an outdoor venue (in whole or in part).	DOD	US Air Force	[7]

Methodology – Phase III

- Proposed definition goes to a broad-based group of participating practitioners and stakeholders
- Online collaboration allows decentralized polling and consensus
- Voluntary consensus standard methodology improves reputability



The Result Is:



- **Consensus Definition**
 - i.e. “An asset is something of value that may be subject to harm or hazard.”
- **Discussion of Definition Context**
 - “In deconstructing existing definitions for asset we find core issues involving Targeting, Protection, Intangibility, Consequence, Ownership, and Types...”
- **Sub-concepts**
 - “Attractive, critical, human, tangible, intangible”
- **Usage**
 - “Used as the component of risk analysis approaches to represent the entity being assessed for protection or other preservative actions...”
- **Concept maps showing process**
 - Diagrams available with a logical online click-through process
- **Historical capture of past usage** (and relationships to current definition)

The Deliverable

- An on-line dictionary of voluntary consensus definitions are then published and released free to Government and Industry for their use
- Periodic review and revision allows future improvement and changes

<http://sarma-wiki.org/index.php?title=Asset>



The Security Analysis and Risk Management Association

P.O. Box 710172
Herndon, Virginia 20171

Phone: 703-635-7906
Fax: 703-635-7935

E-Mail: lexicon@sarma.org
Internet: www.sarma.org