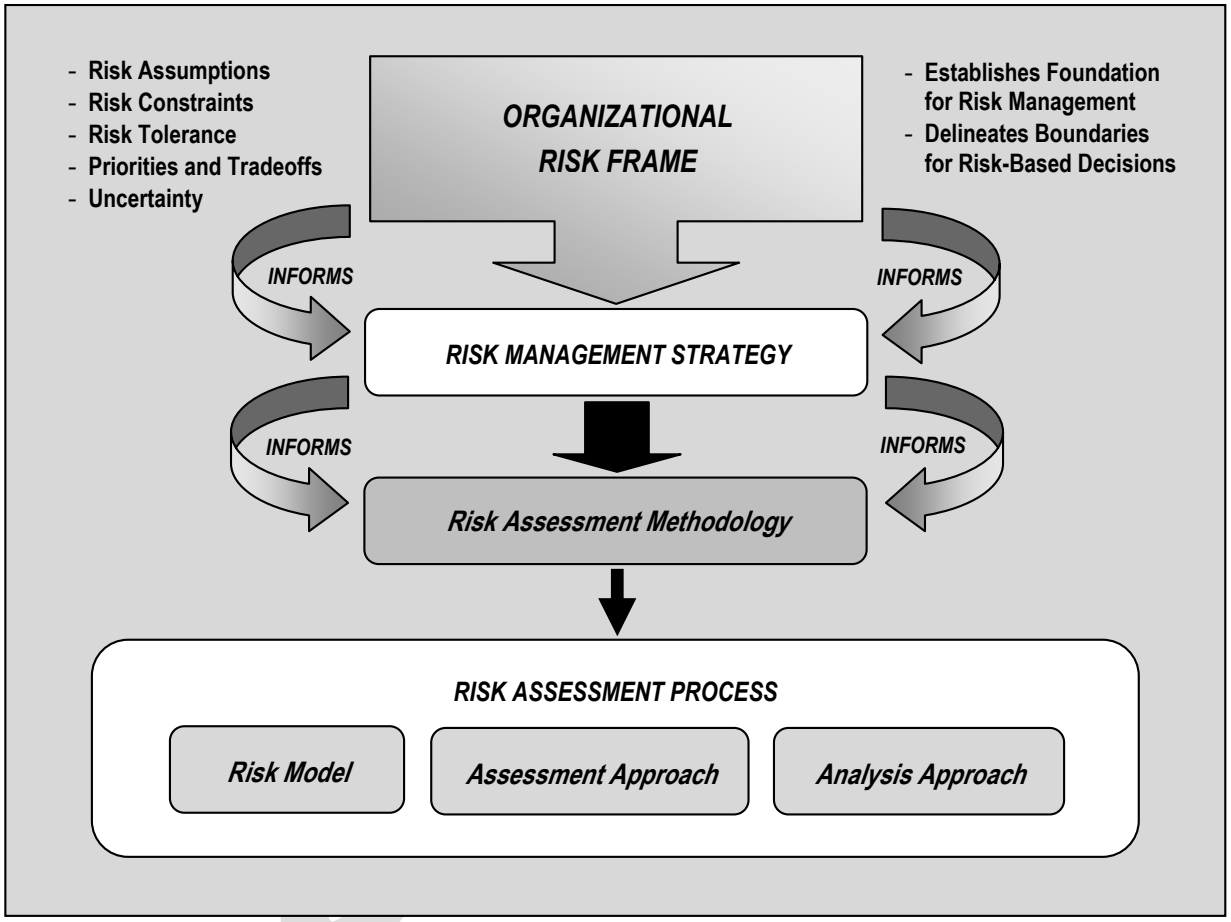
NIST 800-30
Guide to Conducting Risk Assessments

DSSA's selected risk-assessment methodology

Rationale

- The DSSA realized that using a predefined methodology would save time and improve our work product
- We selected NIST 800-30 after reviewing several dozen alternatives
- The reasons we selected this one include:
  - It's available at no cost
  - It's being actively supported and maintained
  - It's widely known and supported in the community
  - It's likely to be consistent with the needs of other parts of ICANN (and thus our pioneering may something that can be "repurposed" elsewhere in the organization)
  - It's available in English

Risk Framing Components



The starting point – framing the analysis

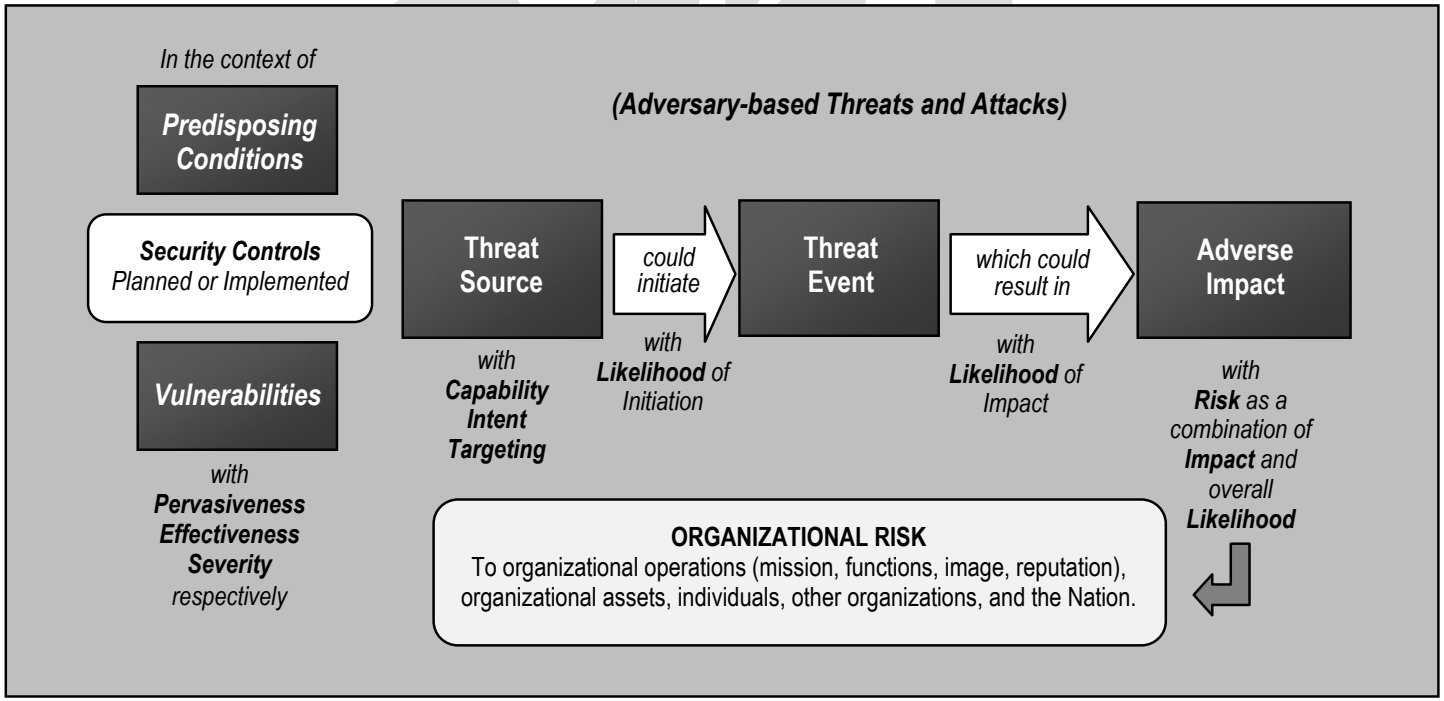
- DSSA is in the midst of a first-iteration of what is likely to be an ongoing process.
- Much of initial framing was done by our Chartering group
- The working group filled in gaps between San Francisco and Singapore

Risk Management Hierarchy

The methodology presumes a tiered approach to the work

- DSSA is chartered to look at the broadest, most general tier
- However we feel it may be useful to pursue one or two deeper, narrower analyses of specific threats once our "survey" work is complete

Adversarial Risk Model

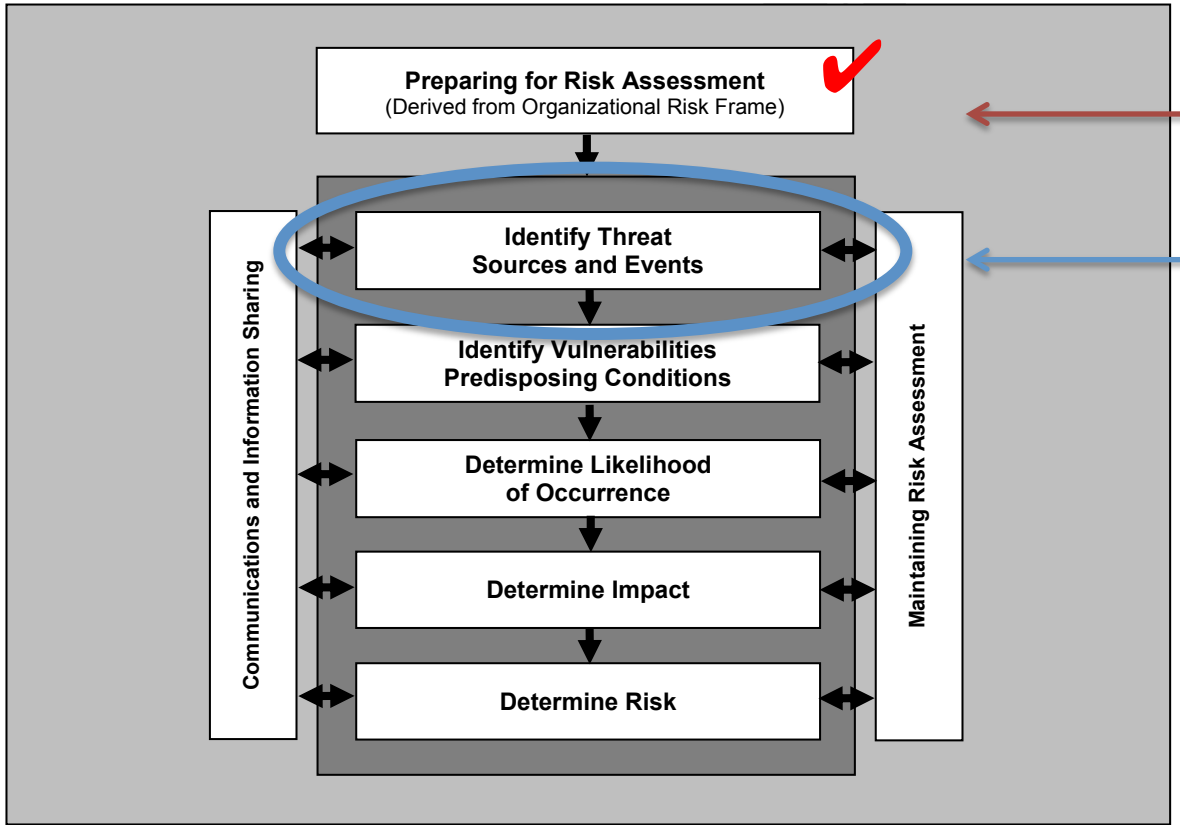


An example of the model – risks from "adversarial" events (which differs from "non-adversarial" threats such as errors, accidents, etc.)

Benefits:

- Consistent terminology
- Shared model
- Structured work
- Sample deliverables

Process overview



Major tasks

- The DSSA feels that the "preparation" work is complete
- We are working on threat-sources and threat-events right now
- This "first pass" through the process is likely to take some time as we learn the methodology and document the threat tree