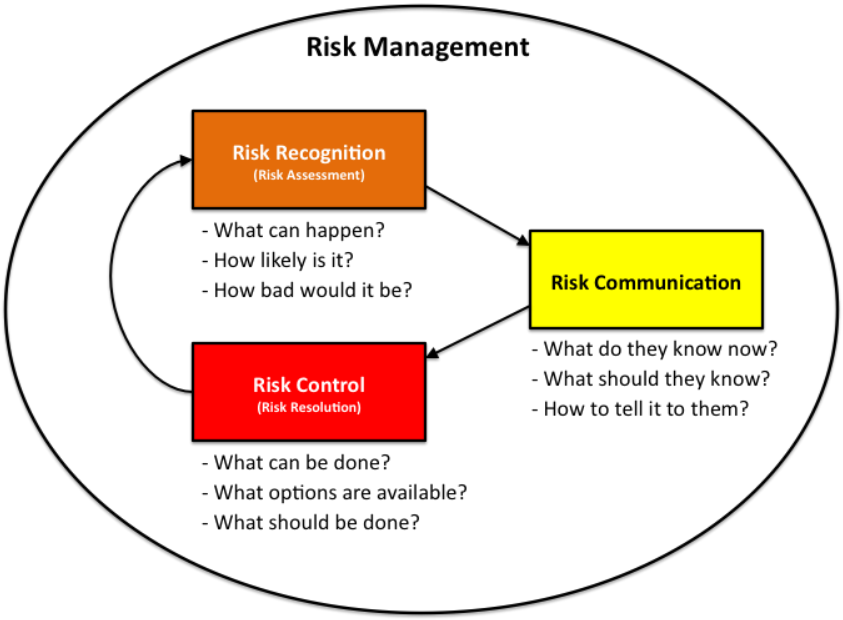
Talking Points: Structured Analysis for Security Risk Management

Will McGill, IST@PENNSTATE, wmcgill@ist.psu.edu

- The Security Risk Management profession can benefit from the use of structured analytic techniques

- SRM consists of three phases, each defined by very specific questions



- "The cornerstone of risk management is understanding." – James Matschulat. Thus, much emphasis is placed on recognizing the risk.

- Understanding is developed in the risk recognition phase, which can be broken down into five different types of activities

    - **Imagine** the risk
    - **Describe** the risk
    - **Observe** the risk
    - **Measure** the risk
    - **Map and Model** the risk

- A number of analytic techniques currently on the books support one or more of these phases. There is sufficient choice to accommodate a range of experience levels and available analytic resources.

- Ultimately, decisions must be made to retain, transfer or mitigate the risk. In the SRM position, the analyst may advise the decision maker or, in some cases, may be the decision maker. The evaluation and monitoring of investment options can also be supported by structured analysis techniques.

- When the analyst plays advisor, he must make the security case via a well-structured argument that clearly highlights what information was used and how it was used. Security Risk Analysts must be held to the same analytic standards described in ICD 203.

- All of this guidance is being packaged into a DHS-funded system that aims to provide analysts of any type with the analytical tools needed to help them better think through their decision problems.