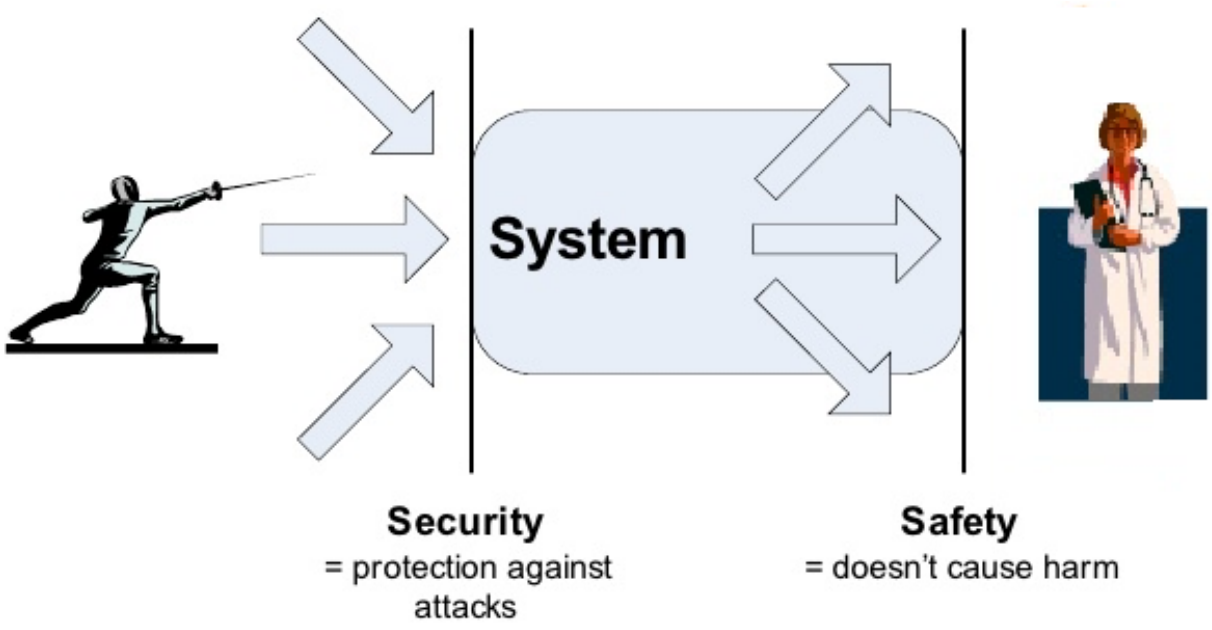
NARSIS Workshop
Training on Probabilistic Safety Assessment for Nuclear Facilities
September 2-5, 2019, Warsaw, Poland

Safety vs Security
(Keynote)

Prof. Behrooz BAZARGAN SABET
BRGM

Safety vs Security

These two concepts are often mixed up
In German, there is just one term for both! « sicherheit »



Safety

is protection against random incidents. Random incidents are unwanted incidents that happen as a result of one or more coincidences.

Security

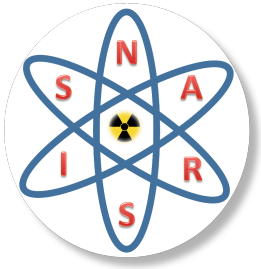
is protection against intended incidents. Wanted incidents happen due to a result of deliberate and planned act.

(Skavland Idsø and Mejdell Jakobsen, 2000)

Safety is about *being protected*, while the **Security** is about *being free from danger*

Vocabulary

Threat	**D**eliberate cause of harm
Likelihood	Potential for an event to harm
Impact	Potential severity of the event
Risk	Likelihood x Impact
Prevention	Reduces likelihood
Mitigation	Reduces impact
Hazard	**N**on-deliberate cause of harm
Vulnerability	Weakness that can allow harm
Residual Risk	The risk remaining after implementation of approved measures



Nuclear safety and nuclear security

In the case of **nuclear safety**, of foremost concern is the radiological risk posed to humans and the environment by human error, equipment failures, internal events (fire, pipe break, etc.) or external events (earthquakes, flooding or other natural catastrophes).

Nuclear security focuses on two main contingencies:
Radiological terrorism and illegal transfer of radioactive material.

A key difference between nuclear safety and security is **intentionality**.
Accidents related to nuclear safety are unintentional, whereas nuclear security incidents are clearly intentional and undertaken with a specific motive.

Contradiction between security of safety in nuclear issues

Nuclear safety and security culture

Safety culture promotes transparency and openness, **Security culture** requires confidentiality.

Safety culture requires that employees share information liberally
Security culture requires that the employees share information with the relevant authorized personnel only.

Emergency response

Nuclear safety requires that the emergency teams should have full access to all areas of facility and to all operations for ensuring safety. **Nuclear security** requires that certain areas should remain secure for security purposes.

During emergency evacuation processes, the main focus of safety personnel is to evacuate all employees as soon as possible; however, for security personnel, identifying and detaining intruders is of utmost importance

Barriers

The main function barriers is to delay the access to the vital areas of a nuclear power plant. For the emergency response team such barriers could inhibit access to critical areas within a facility in the event of an accident

Access control

For the **safety** point of view, facilitated access is required to all the places at the facility. However, the access to many vital areas may be required to be under access control for **security** purposes.
During normal operations some areas within a reactor facility may be subject to special physical protection systems, however, in case of emergency these areas should be accessible to facilitate evacuation of personnel.

Transport of nuclear material

Safety procedures may slow the transport of materials, while the application of **security** regulations may require minimization of the time duration of transport.
For nuclear **safety**, any transport vehicle is required to make the public aware that nuclear material is being transported. Nuclear **security** dictates confidentiality to avoid opportunity to commit an act of nuclear sabotage.

Similarity and divergence

Responsibility and regulation

regulations governing safety and security are necessary different. The prime responsibility for safety lies with the operator of a facility. The issues of security are related to the regalian role of the states.

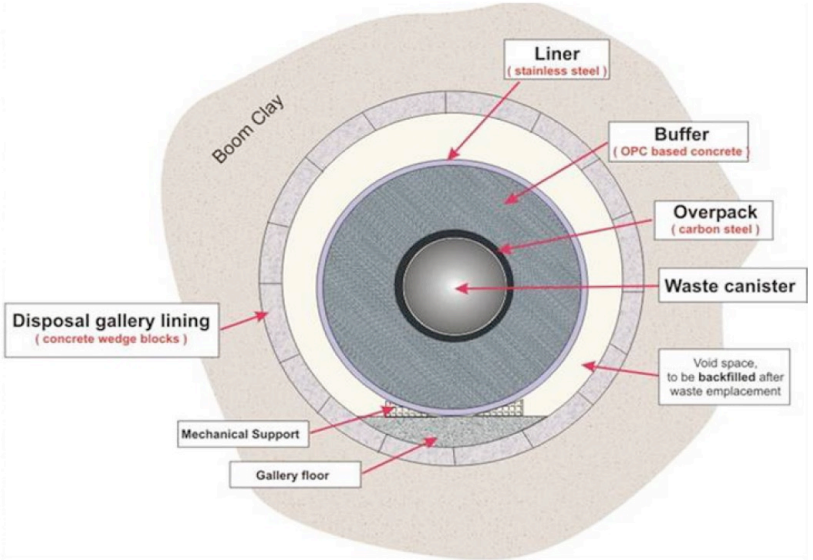
Design criteria

Design concepts like defense-in-depth, redundancy, passive systems, etc applied to nuclear safety are applicable to nuclear security too.

Defense-in-depth

In the case of nuclear **safety**, defense-in-depth is implemented by creating multi-barriers Defenses against the release and the movement of radioisotopes.

In nuclear **security**, various layers of protection are implemented at various physical boundaries such as Main Plant Boundary, Operating Island, vital areas etc. in a graded approach.



Multi-barrier disposal, Belgium concept

Source CEN-SCK

Design criteria *(cont.)*

Basis of design

In the case of safety, the basis of design of a nuclear power plant is the Design Basis Accident (DBA). A DBA is ‘‘a postulated accident that a nuclear facility must be designed and built to withstand loss to the systems, structures and components necessary to ensure public health and safety’’. In nuclear security, Design Basis Threat (DBT) serves as a benchmark for the design of physical protection systems for nuclear power plants.

While DBA’s remain the same throughout the life of the facility, DBTs evolve and may change as the security threat changes with time. while DBA document is open to public, DBT is a confidential in nature.

Passive systems

Passive systems, increase robustness of nuclear safety by minimizing human intervention and hence, minimizing the margin for human error. Security passive systems are related to automatic devices such as HD remote cameras, speakers, and video analytics.

Training and education

Training is a common requirement for nuclear safety and security issues. Unlike nuclear safety, nuclear security is usually not covered in the traditional training curriculum for nuclear engineers and scientists.


SAFETY


SECURITY


Identify
Assess
Risk
Management
Treat
Monitor

Probabilistic Security Assessment
(VESPA approach, Cipollaro 2015)

In its simplest formulation risk (R),, can be defined as the probability (P) that an event produces a given consequence (C), times C itself.

$$R = P.C$$

For an adversary with the intention to create a consequence of a given severity (S), the risk constitutes an opportunity (O), which is proportional to the plausible likelihood (L) that this opportunity is used to create a sabotage act in order to induce a damage of given severity and consequences (S).

$$O \propto L.S$$

The likelihood that a Physical Protection System (PPS) might fail depends on the probability of being subject to a challenge (Pa) and the complement of the probability to respond to it (Pr). The typical approach is that the risk is estimated on condition that an **attack will certainly occur**. And then Pr is assessed based on the physical security strategy in place (defence-in-depth, deterrence, detection, delay and response principles, etc.).

$$P = Pa.(1 - Pr)$$

$$L \propto \frac{P}{1-Pr} = Pa$$

(L) can be regarded as being related to the probability of attack to the facility, which can in turn be seen as representing the PPS failure probability.

Cipollaro, A., 2015 Ph.D. thesis,. University of Pisa.

The focus is put not on the dimensioning of the PPS but on estimating the plausibility of an attack. Therefore:

$$L \propto Pa = f\{A, F\}$$

A: attractiveness indicating of the extent to which malicious act fits the adversary objectives
F: Feasibility level expressing difficulty to exploit a given vulnerability.

By defining a set of parameters selected as relevant (L) metrics , it is possible to establish a comparative rating of certain plausible scenarios.
Such parameters are for instance:

- General threat environment: the level of exposure to sabotage
- Potential for socio-economic disruption
- Vulnerability versus Plant operational states
- ect…

Act that is very attractive but too complex to be feasible would score low, as well as one relatively feasible but not attractive.

Risk Matrix

RISK MATRIX		IMPACT				
LIKELIHOOD		NEGLIGIBLE	MINOR	MODERATE	SEVERE	CRITICAL
	VERY LIKELY	LOW	MEDIUM	HIGH	VERY HIGH	
	LIKELY	LOW	MEDIUM	HIGH	HIGH	VERY HIGH
	MODERATELY LIKELY	LOW	LOW	MEDIUM	HIGH	HIGH
	UNLIKELY	LOW	LOW	LOW	MEDIUM	MEDIUM
	VERY UNLIKELY	LOW	LOW	LOW	LOW	LOW

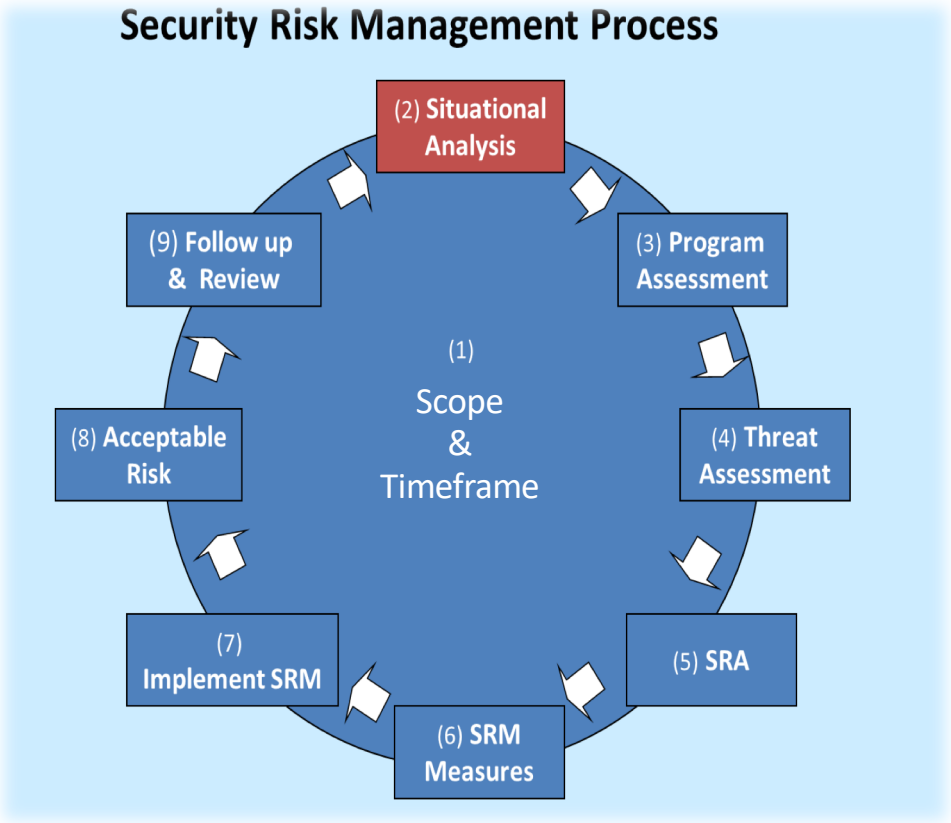
Security Risk Management Process

(UN)

Setting scope and timeframe

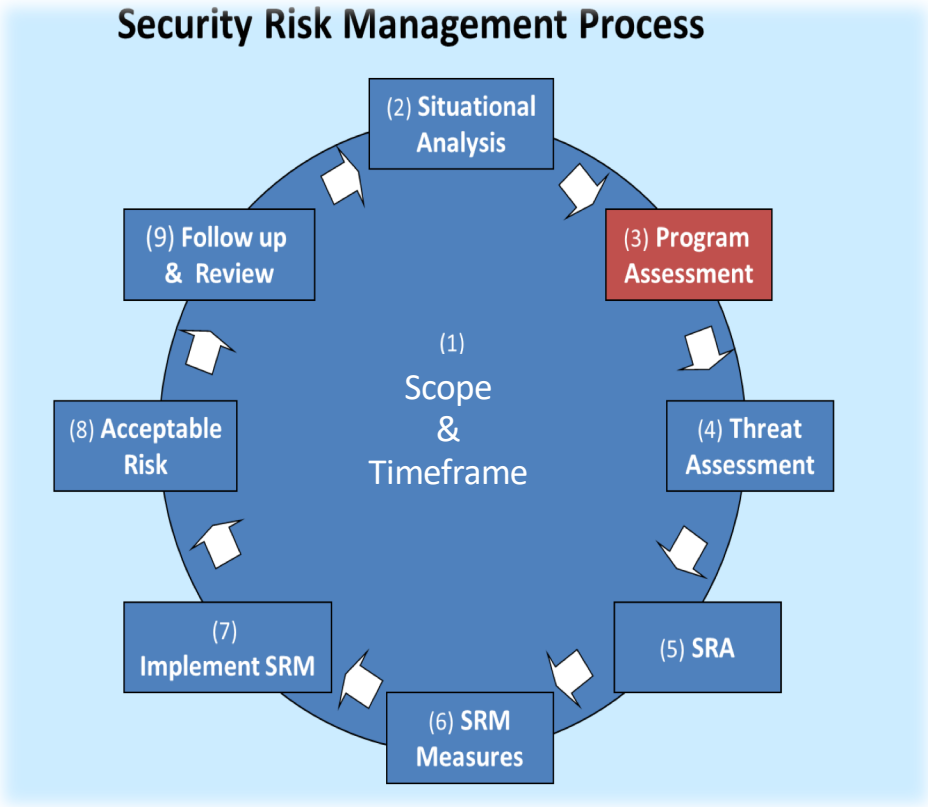
- **Where will we be working and what is the timeframe for the actions?**

Step 2
Situational Analysis



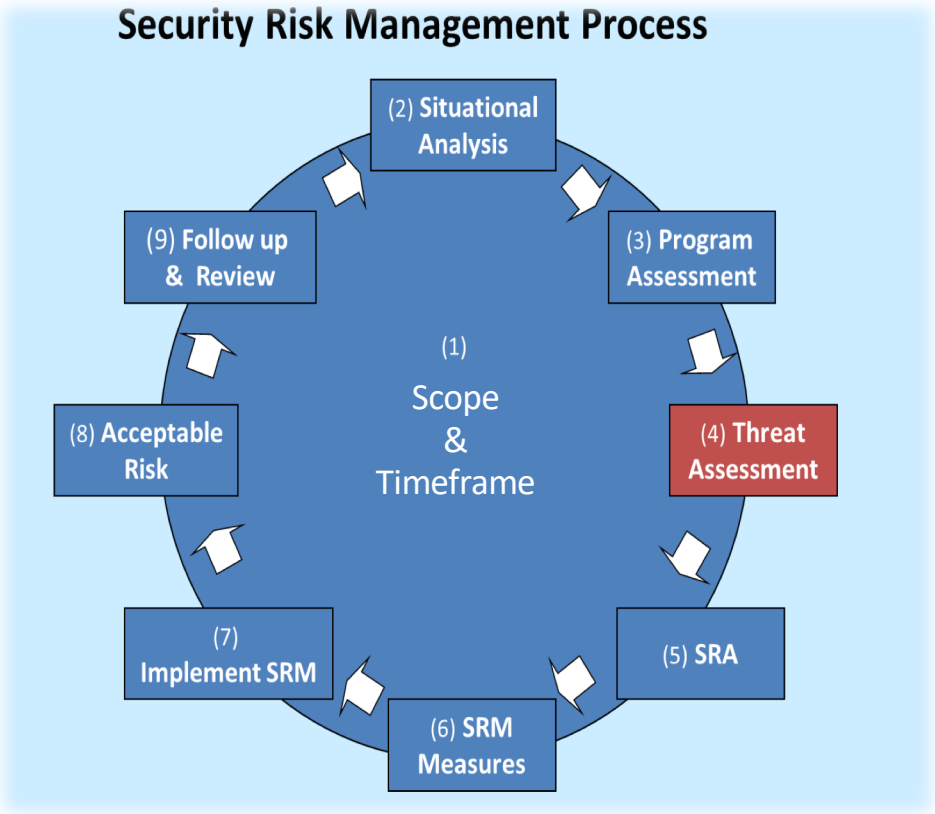
- **What is the overall security situation in that area?**

Step 3
Programme Assessment



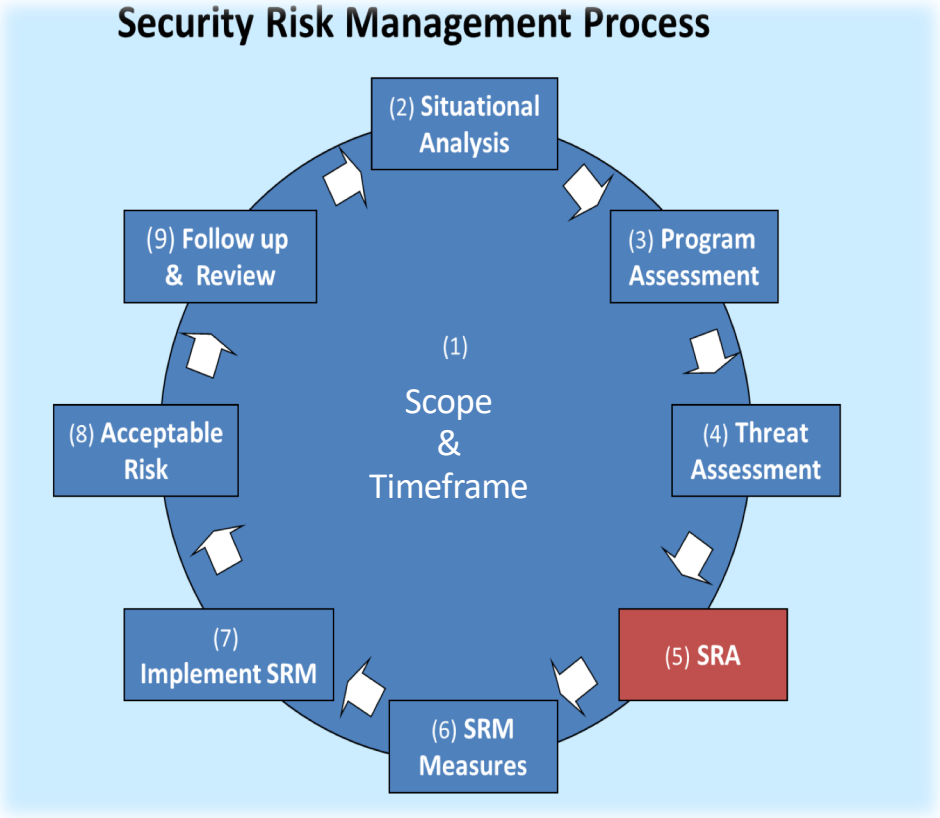
- **What are the main program/ activities' goals in that area?**

Step 4
Threat Assessment (General & Specific)



- **What are the obstacles to achieving goals?**

Step 5
Security Risk Assessment

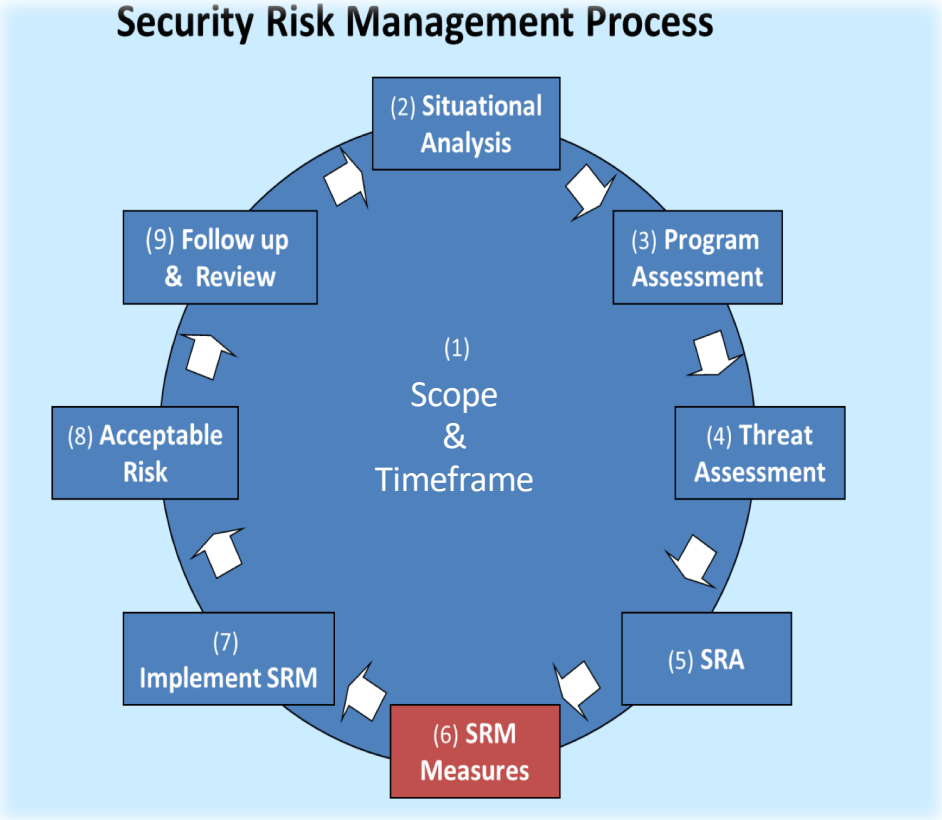


- **How vulnerable is the Organization to these threats?**
- **How will they affect the Organization, and which threats require the most attention?**

Risk Matrix

RISK MATRIX		IMPACT				
LIKELIHOOD		NEGLIGIBLE	MINOR	MODERATE	SEVERE	CRITICAL
	VERY LIKELY	LOW	MEDIUM	HIGH	VERY HIGH	
	LIKELY	LOW	MEDIUM	HIGH	HIGH	VERY HIGH
	MODERATELY LIKELY	LOW	LOW	MEDIUM	HIGH	HIGH
	UNLIKELY	LOW	LOW	LOW	MEDIUM	MEDIUM
	VERY UNLIKELY	LOW	LOW	LOW	LOW	LOW

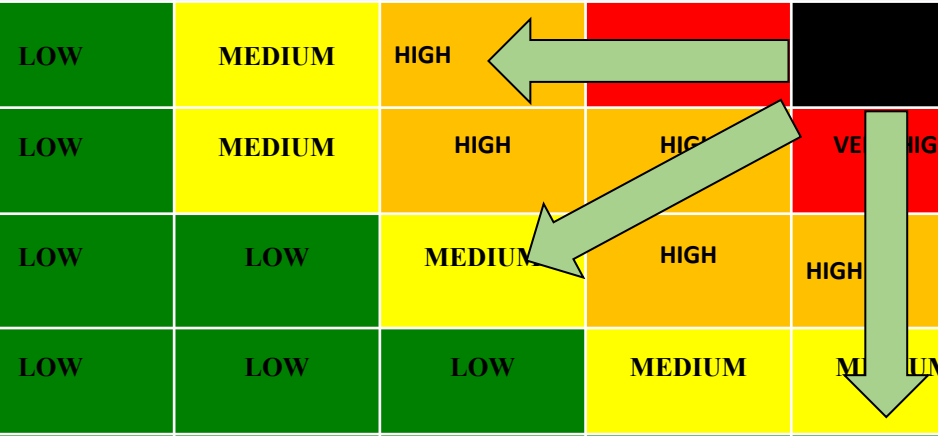
Step 6
Security Risk Management Decisions



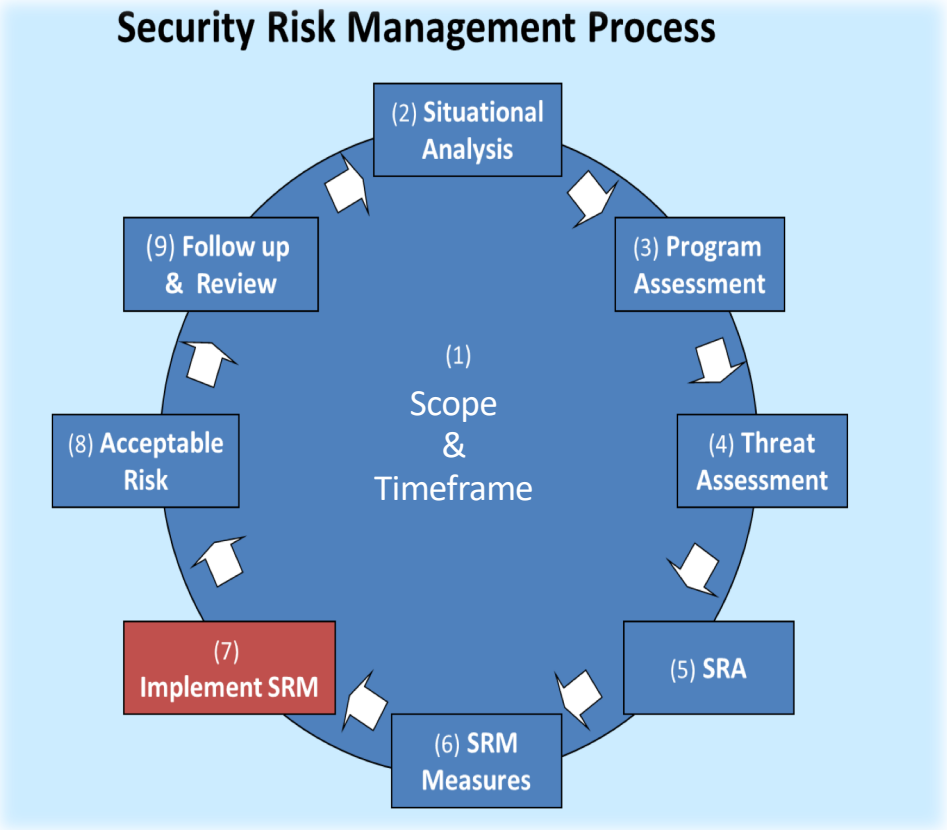
- **What can actually be done about these risks?**

Risk Matrix

RISK MATRIX		IMPACT				
LIKELIHOOD		NEGLIGIBLE	MINOR	MODERATE	SEVERE	CRITICAL
	VERY LIKELY	LOW	MEDIUM	HIGH		
	LIKELY	LOW	MEDIUM	HIGH	HIGH	VE IGH
	MODERATELY LIKELY	LOW	LOW	MEDIUM	HIGH	HIGH
	UNLIKELY	LOW	LOW	LOW	MEDIUM	M UM
	VERY UNLIKELY	LOW	LOW	LOW	LOW	LOW



Step 7
Security Risk Management Implementation



- **Procedural and budget aspects of implementing the agreed security risk management measures**

Step 8
Acceptable Risk

- **Is the risk acceptable in balance with the criticality of program activities?**

Step 9
Follow up and Review

- **Are the measures working?**
- **Is the assessment of risk now similar to how it was projected?**

One who knows and knows that he knows...

His wisdom will reach the skies!

One who knows, but doesn't know that he knows...

He is asleep, he should be wake up!

One who doesn't know, but knows that he doesn't know...

His limping mule will eventually get him home!

One who doesn't know and doesn't know that he doesn't know...

Fakhr Al-Din Mahmud Ibn Yamin

He will be eternally lost in his forgetfulne