The ETSI TISPAN Security Evaluation Method TVRA - Threats Vulnerability Risk Analysis:

ETSI TISPAN WG7- NGN Security Architecture - has developed and published in ETSI TS 102 165-1[TVRA] the new method and proforma for the evalution and analysis of "Next Generation Networks" due to threats, risks and vulnerabilities.

One of the identified roles - within standards domain - is "to give justification for the development of standards based on security solutions" [TVRA Sec.4.1].

Another identified role - within domain of Protection Profile (PP) [see ISO Standard Common Criteria] Generating - is to give guidance for the derivation of security-related content from protocol or any other service specification.

The security analysis process is a cyclic process encompasing security objectives (assurances), security requirements and a related security architecture (mechanisms) of a system respectively standard considered.

The security analysis process is cyclic due to the continuous changing triggered by any internal or external behaviour to the system.

On Security Objectives - Requirements - Architecture (Sec-ORA) a vulnerability analysis with respect to possible threats must be carried out. When an anticipated security assurance level (SAL) by applying refined countermeasures cannot be reached, TVR-Analysis processing continues until the SAL is sufficiently being approximated.

The vulnerability analysis is a metric of the attack-potential of a system measuring the factors of expertise, openness, availability of resources that make a system vulnerable to attackers.

The design of a system takes the system assets into focus by considering the system objectives. System Objectives contain Security and Assurance(S/A) Objectives. Since objectives implement requirements, system objectives must implement system+ security+ assurance+ requirements.

A TVR-Analysis is said to be complete, iff both are examined in-depth, i.e.

1. the system modules with respect to its system objectives comprising all system+ security+ assurance requirements;
2. the system assets with respect to its identified attack potential to the system environment.

A weighted TVR-Analysis of the system yields the the risk to assets due to its associated vulnerabilities which are occasionally triggered when exploiting unwanted incidents. Of course, the purpose of analysis is to minimize probability of any instance from the class of unwanted incidents.

Vulnerability Analysis of an asset comprises identification of its weaknesses and of specific attacking threats enacted by threat agents.

Attacking threats can be classified according to security weaknesses they try to exploit:

1. interception of communication
2. manipulation of data or messages

3. denial of service
4. repudiation of sending or receiving agents
5. botnetted/unauthorized service subscription

Security Objectives can be classified according to security capabilities to be exploited when minimizing risks:

1. confidentiality of communication
2. integrity of data or messages
3. availability of services
4. authenticity of sending and receiving agents
5. accountability of subscribed services

Security weaknesses and security capabilities are combined into the so-called TVRA Object/Data Model (DOM) comprising the two enumeration types of threats and of security objectives with above related 5 elements each type.

In systems countermeasures are strategically applied, i.e. to lower likelihood of unwanted incidents arising. Likelihood depends from presence of security weakness of an asset and from threats enacted by threat agents trying to exploit security weaknesses. Thus countermeasures have the purpose of remove or mask the weaknesses of an asset by technical or non-technical [see ISO7001, ISO17799] measures.

Non-technical measures mean redesign and hardening of assets:

1. asset redesign anticipates the removal of an inherent weakness based on the security analysis assuming there is no asset without weakness.
2. asset hardening anticipates masking or inaccessible-making of weaknesses that cannot be removed.