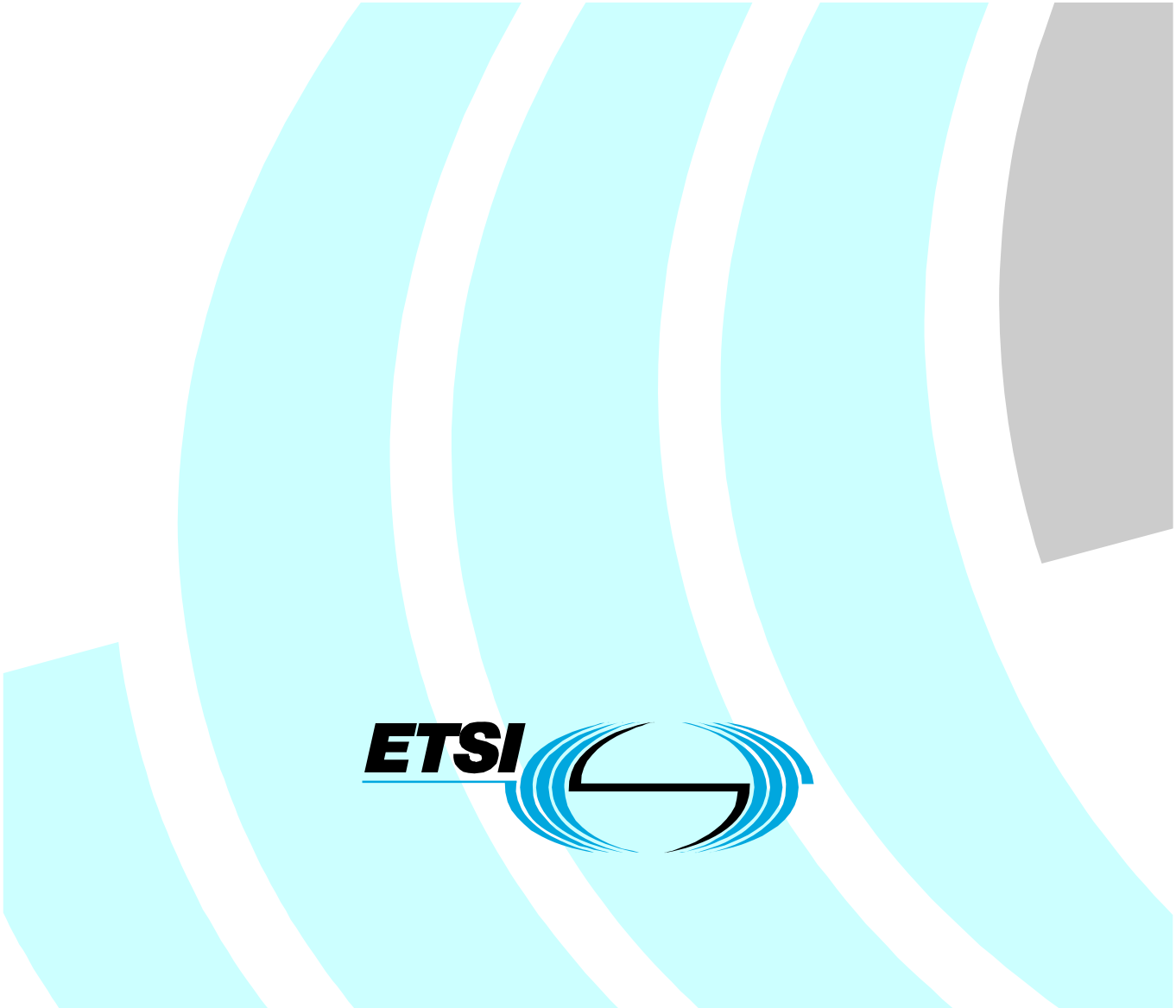
ETSI TR 187 014 V2.1.1 (2009-02)

Technical Report

Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); eSecurity; User Guide to eTVRA web-database



Reference
DTR/TISPAN-07020-NGN-R2

Keywords
data, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://webapp.etsi.org/IPR/home.asp).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN).

1 Scope

The present document is a guide to the use of the ETSI eTVRA web-application.

NOTE: The eTVRA web-application acts as a tool for entering analysis results following completion of an analysis using the ETSI TVRA method defined in TS 102 165-1 [i.1].

2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific.

- For a specific reference, subsequent revisions do not apply.
- Non-specific reference may be made only to a complete document or a part thereof and only in the following cases:
  - if it is accepted that it will be possible to use all future changes of the referenced document for the purposes of the referring document;
  - for informative references.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

2.1 Normative references

The following referenced documents are indispensable for the application of the present document. For dated references, only the edition cited applies. For non-specific references, the latest edition of the referenced document (including any amendments) applies.

Not applicable.

2.2 Informative references

The following referenced documents are not essential to the use of the present document but they assist the user with regard to a particular subject area**.** For non-specific references, the latest version of the referenced document (including any amendments) applies.

[i.1] ETSI TS 102 165-1: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis".

[i.2] ETSI TR 187 011: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Application of ISO-15408-2 requirements to ETSI standards - guide, method and application with examples".

[i.3] ISO/IEC 15408-2: " Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional components".

[i.4] ISO/IEC 15408-1: "Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model".

[i.5] ISO/IEC 15408-3: "Information technology - Security techniques - Evaluation criteria for IT security - Part 3: Security assurance components".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in TS 102 165-1 [i.1] and TR 187 011 [i.2] apply.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

EAL	Evaluation Assurance Level
EOL	ETSI On Line account
TVRA	Threat Vulnerability and Risk Analysis
UML	Unified Modelling Language
URL	Uniform Resource Locator

4 Overview of eTVRA web application structure

The eTVRA web application is structured as shown in figure 1.

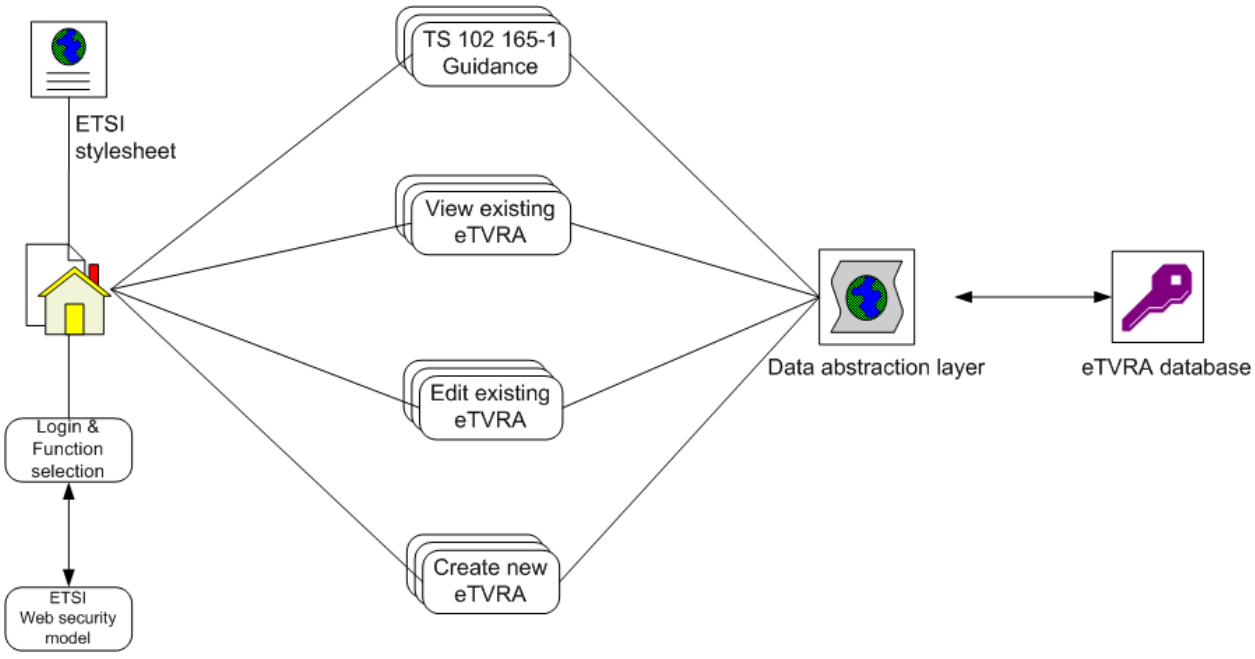


Figure 1: eTVRA web application structure

The web page design is aligned to the "look and feel" of the ETSI Web-application suite and any change to the overall ETSI look will be reflected in the eTVRA site.

The eTVRA tool and website populates a database, as defined in annex E of TS 102 165-1 [i.1] but modified for practical implementation on the ETSI server platform. The eTVRA site and database allow cataloguing of the results of the analysis but does not present any shortcut in the analysis (although it may be possible to modify entries and their associated risk to view the impact of adding countermeasures to the system).

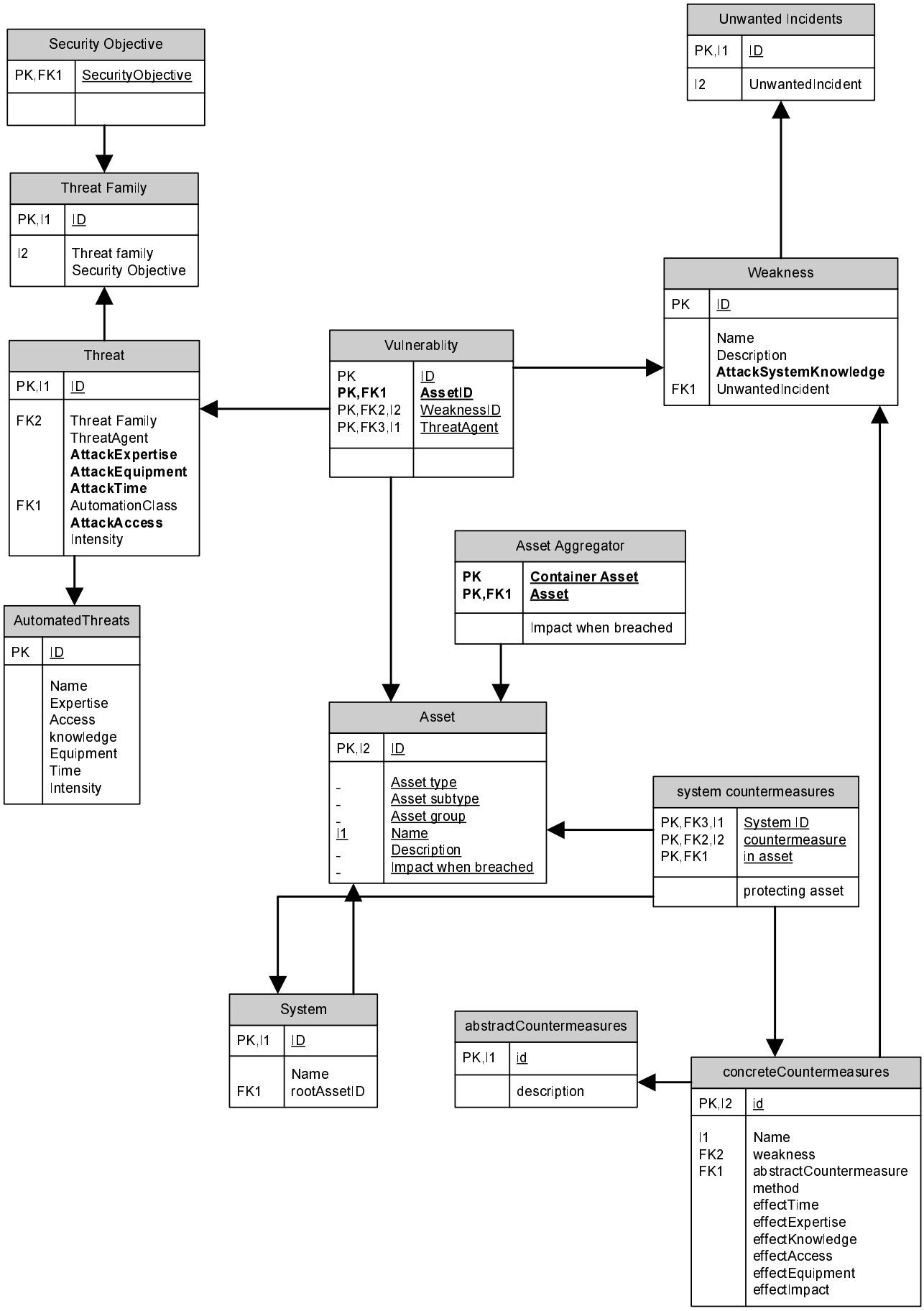


Figure 2: Database structure extracted from MS-Access™ TVRA test database

5 User guide

5.1 Access to the eTVRA home page

The ETSI TVRA homepage is accessed via the following URL:

http://portal.etsi.org/eTVRA/

NOTE: The eTVRA site is noted as under construction and the present document is a guide to the current version of the site. Feedback garnered through its operation will be used to improve and modify the site in a future release.

Figure 3: eTVRA website welcome page

5.1.1 Access restrictions

Access to the eTVRA application is restricted in the following way:

Table 1

Role	Access
EOL account holders	Read only access to database content
eTVRA administrator	Full access to the database
ETSI support	Access to update webpages

On entering the eTVRA site the user will be directed to enter the EOL account user-name and password. If a TVRA user does not have such credentials they have to be requested from ETSI. EOL accounts may be applied for online from the following URL:

http://webapp.etsi.org/createaccount/

5.2 eTVRA step 1

5.2.1 Creation and editing systems

The first step defined for the eTVRA is identifying the objectives. As a pre-requisite it is essential to first define the system itself.

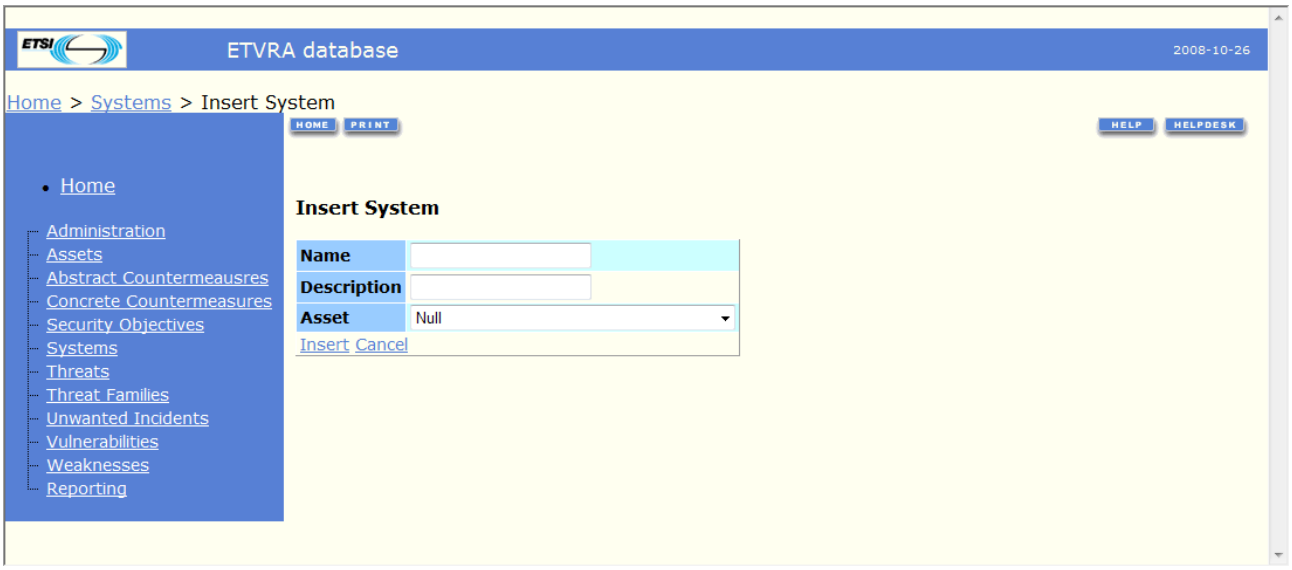


Figure 4: Screen shot for entering a system

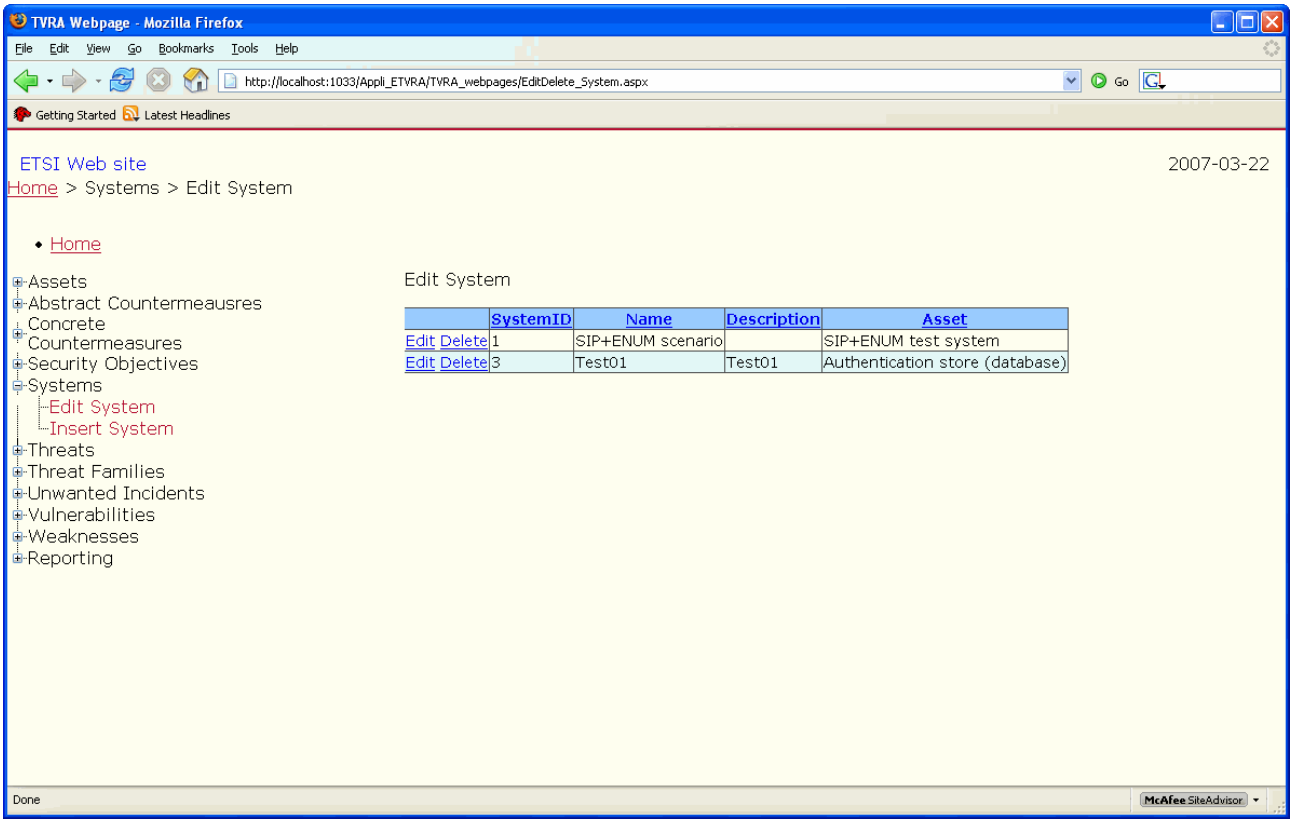


Figure 5: Screen shot for editing a system

5.2.2 Creation and editing of objectives

As stated in TS 102 165-1 [i.1] the objectives for security are the essential starting point of the design. Should these objectives be unclear or *unconsciously* changing during the design process the system becomes more difficult (and hence expensive) to secure. Alternatively, if the objectives are not clear from the outset of the design important security aspects may be left unaddressed that may lead to costly incidents and/or repair operations.

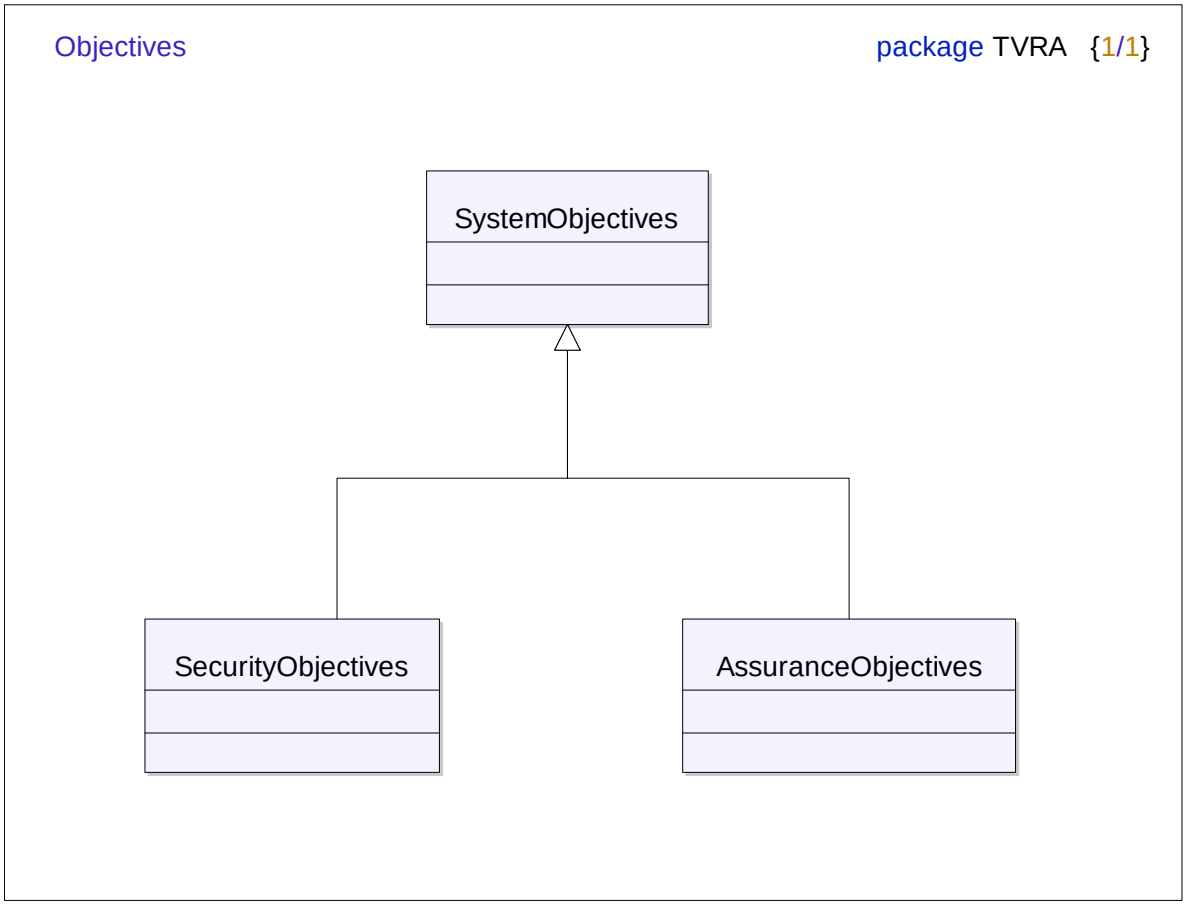


Figure 6: Hierarchy of objectives in a system design

As shown in figure 6 assurance objectives and security objectives are specializations of system objectives. Those characteristics of an objective that mark it out as a security objective are those that refer to one or more of the following system attributes:

- Authenticity.
- Confidentiality.
- Availability.
- Integrity.

Within the context of standardization there are a number of objectives for security that are intended to ensure availability of the network and customer confidence. These objectives break down to the following technical security issues for most telecommunications services:

- charging fraud;
- protection of privacy; and
- ensuring availability of the offered services.

The goals for telecommunications services should therefore aim to reduce these risks by reducing the ability to mount attacks that prevent the achievement of these objectives.

The following technical objectives for telecommunications services security hold:

- Prevention of masquerade:
  - being able to determine that a user claiming to be Alice is always Alice, Bob is always Bob, and Bob cannot pretend to be Alice;
  - applies to both masquerade of the user and of the system or service.
- Ensure availability of the telecommunications services:
  - the service must be accessible and usable on demand by an authorized entity.

NOTE: In general, a user expects to be able to place a call, and complete the call without being cut off in the middle.

- Maintain privacy of communication:
  - where the parties to a call communicate across public networks mechanisms should exist to prevent eavesdropping;
  - the only delivery points for communication have to be the legitimate parties to the call.

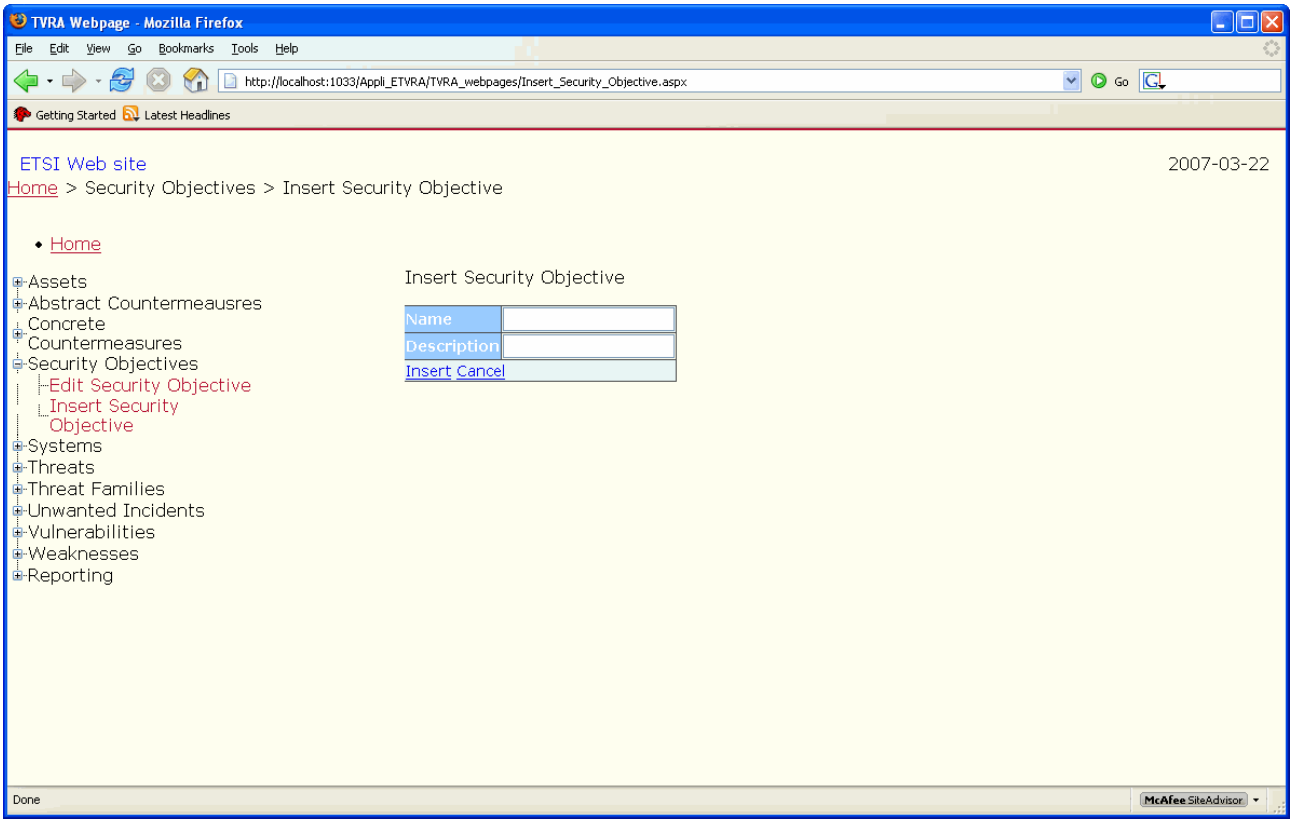


Figure 7: Screen shot for entering an objective

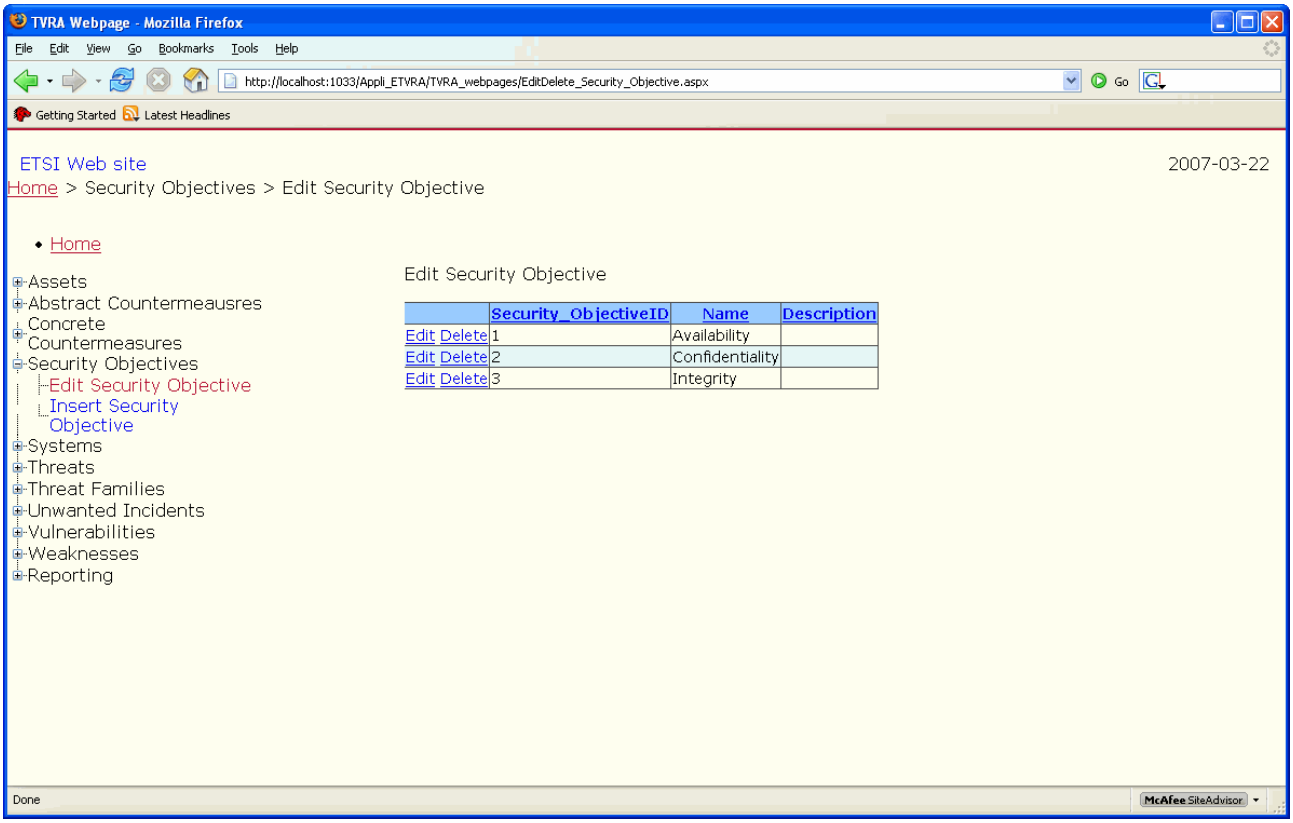


Figure 8: Screen shot for editing an objective

5.2.3 Creation and editing of unwanted incidents

Unwanted incidents are the corollary of objectives, whereas an objective is stated as an intent, an unwanted incident is stated as something the designer explicitly does not want the system to do.

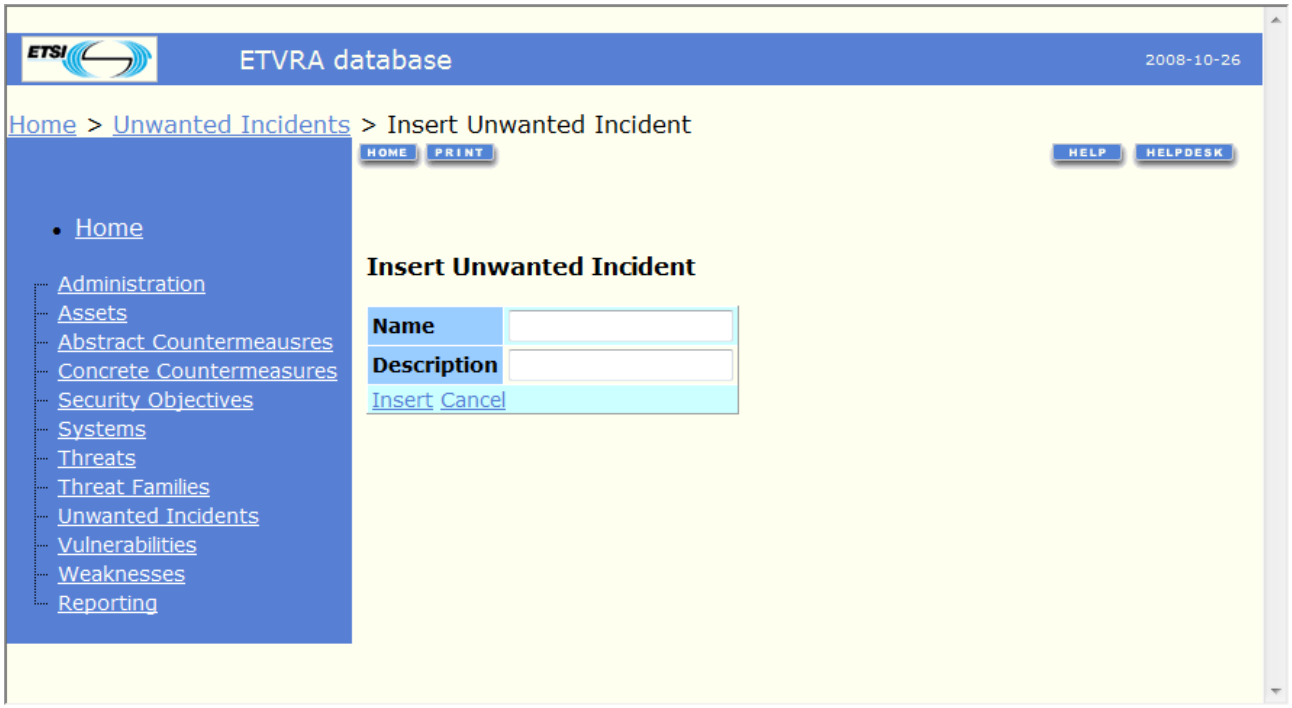


Figure 9: Screen shot for inserting an unwanted incident

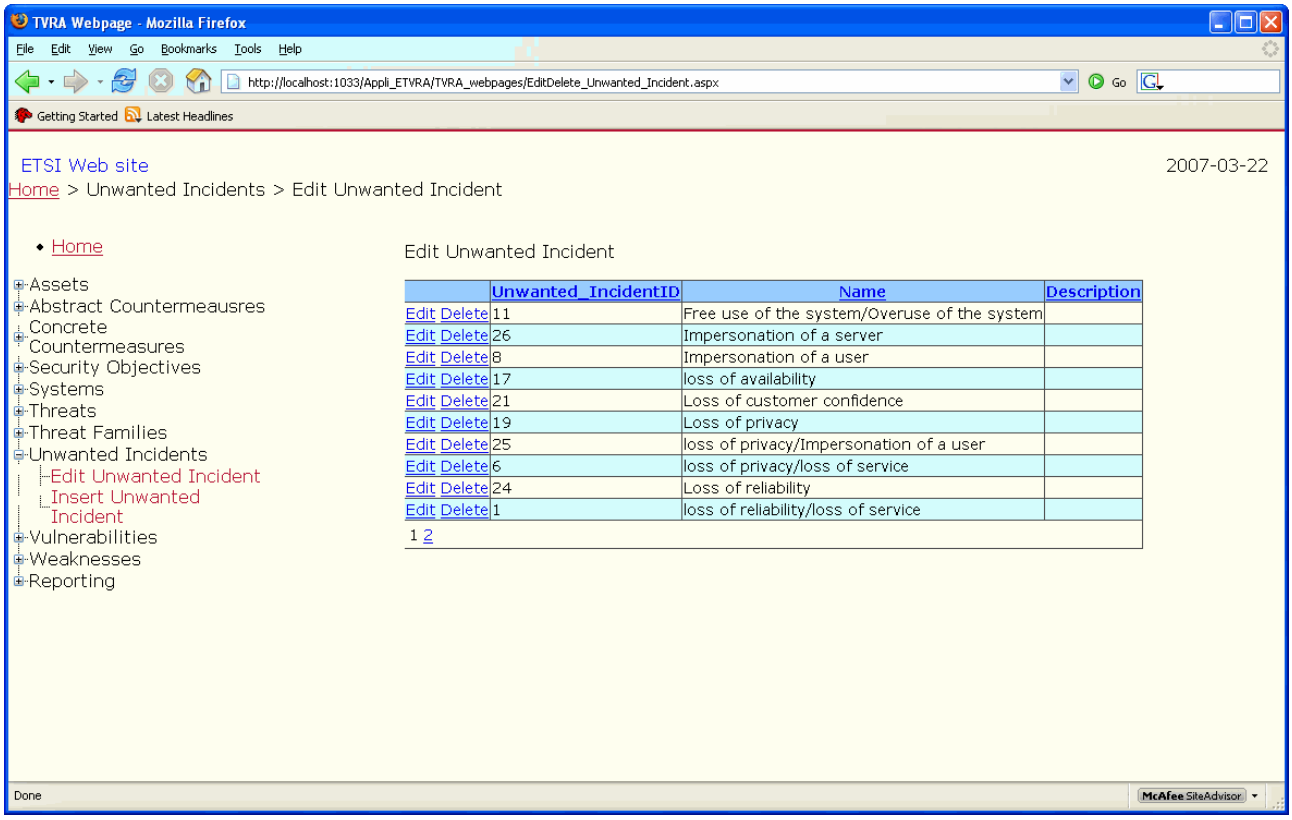


Figure 10: Screen shot for editing an unwanted incident

5.3 eTVRA step 2

The system requirements are dependent on the system objectives identified in step 1 and have two specialisms shown in figure 11 identifying security and assurance requirement specialisms.

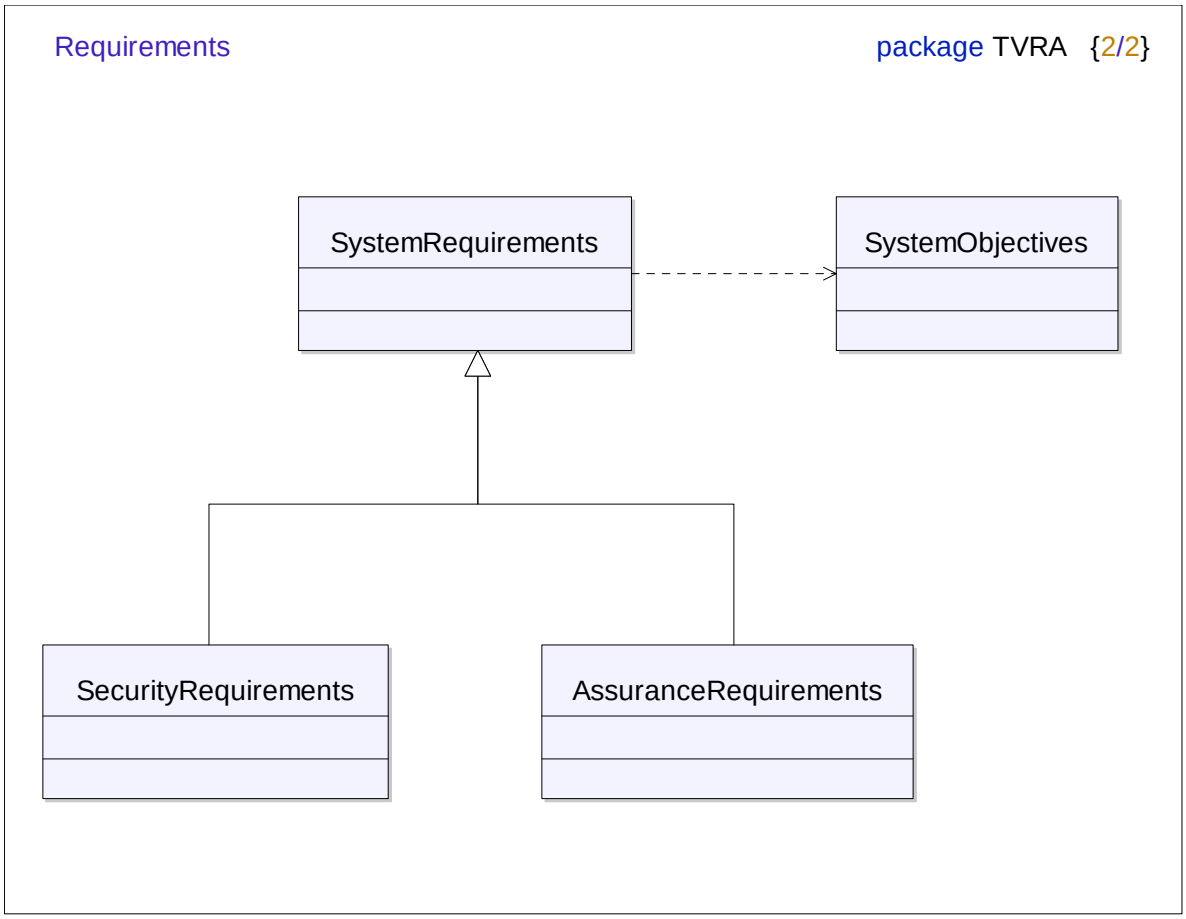


Figure 11: Dependency relationship between requirements and objectives

Following the guidance given in TR 187 011 [i.2] security functional requirements should be defined using the model specified in ISO/IEC 15408-2 [i.3] and should be specified for both the asset and, where applicable, its environment. The asset security functional requirements should be classified into the following groups:

- asset security functional requirements:
  - an identification the security functional requirements as specified by reference to the functional components defined in ISO/IEC 15408-2 [i.3] where the assignments and/or selections required have been made for the system under evaluation;
- asset security assurance requirements:
  - an indication of the Evaluation Assurance Level (EAL) as described in ISO/IEC 15408-1 [i.4] that an implementation of the base security standard could be expected to meet. As there are likely to be many implementations in a number of different application areas, the EAL requirement could be expressed as a range (e.g. EAL3 - EAL5);
  - where possible, an identification of any specific assurance components from ISO/IEC 15408-3 [i.5] which will apply to an implementation; and
  - where necessary, a specification of any essential assurance requirements which are not included in ISO/IEC 15408-3 [i.5].

When building systems the use of ISO/IEC 15408-2 [i.3] functional capabilities offer a means to unambiguously state requirements. Requirements are modelled further in the system as specific assets although this may be revisited.

NOTE: The eTVRA tool and method in its current form does not allow a simple guided means of linking system assets, objectives and requirements. This should be updated.

5.4 eTVRA step 3

TS 102 165-1 [i.1] identifies step 3 as the systematic identification and cataloguing of assets and recommends the use of UML use case diagrams, class diagrams and object diagrams to assist in the analysis of the system to identify the assets. In the course of cataloguing the assets the following attributes and relationships have to be identified:

- The system in which the asset resides.

NOTE 1: An asset may exist in more than one system and a system may contain many assets (a many to many relationship).

- The asset parent-child-sibling relationships if any exist.

NOTE 2: An asset may be a parent to one or more other assets and such relationships have to be captured. Similarly an asset may be a peer (sibling) to another asset and such relationships have to be captured.

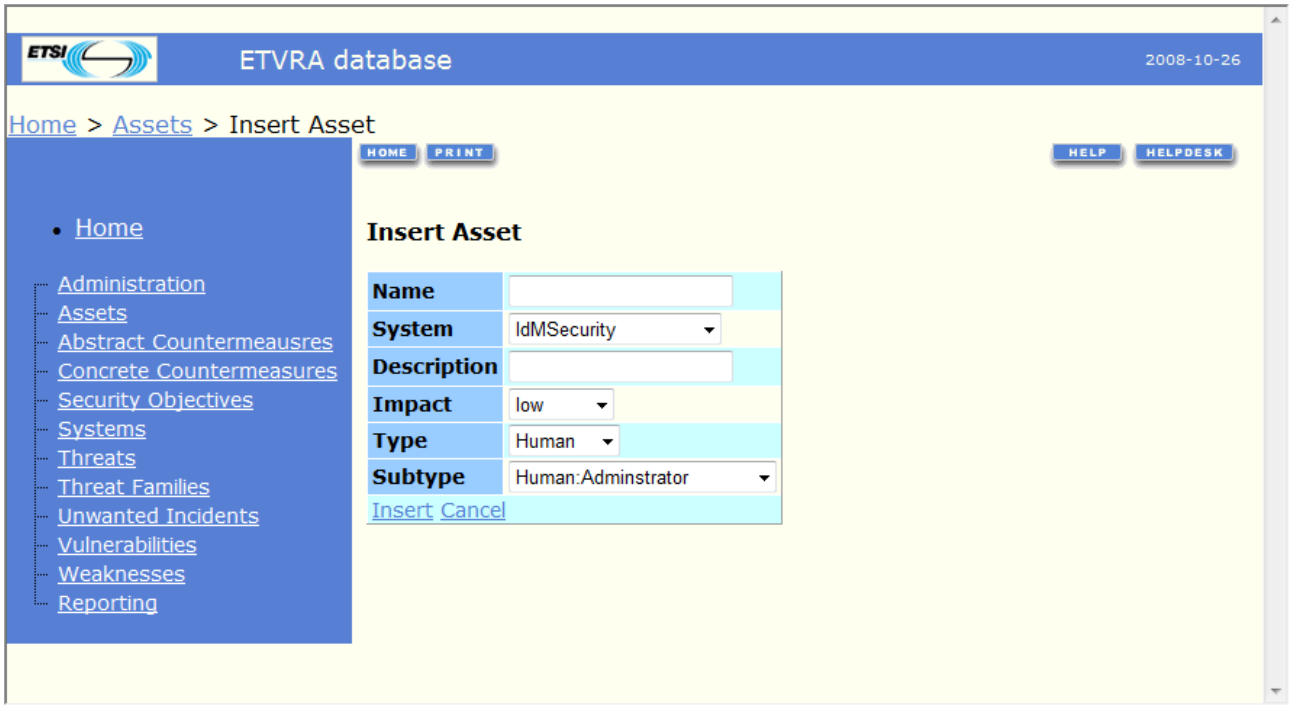


Figure 12: Screen shot for adding an asset

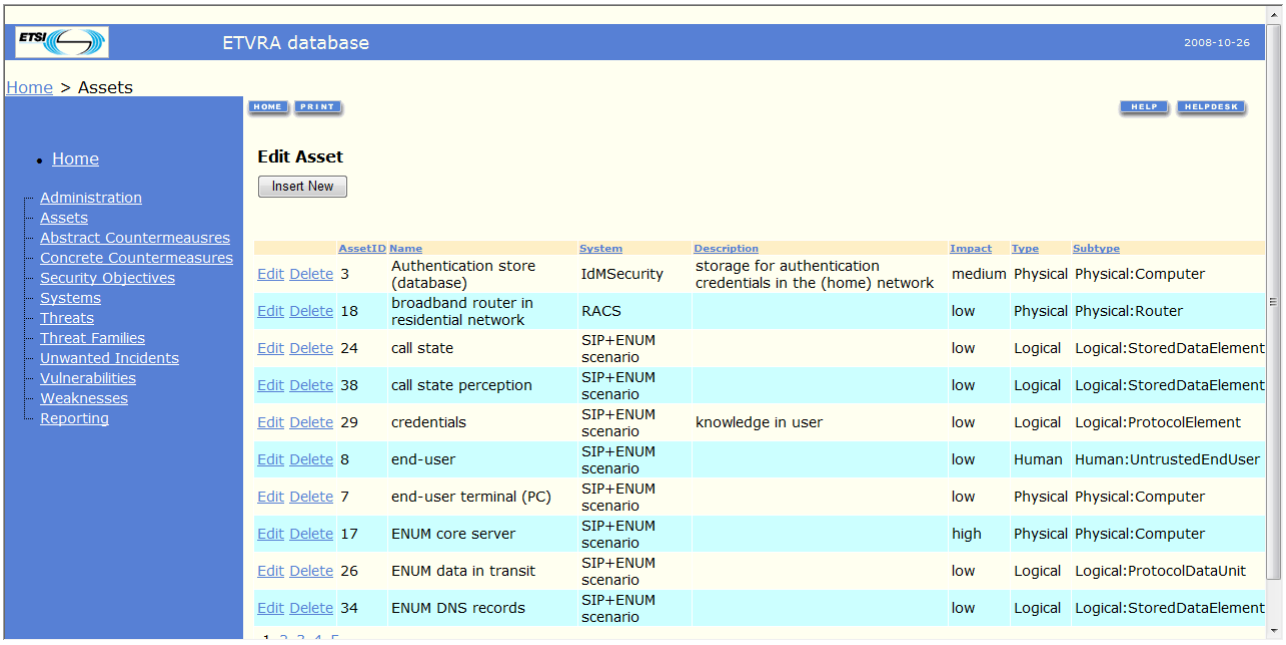


Figure 13: Screen shot for editing an asset

5.5 eTVRA steps 4, 5, 6 and 7

The description in TS 102 165-1 [i.1] breaks step 4 into a number of closely aligned sub-tasks.

- Step 4.1: Identification of vulnerability.
- Step 4.1 a: identification of weakness:
  - The weakness provides the attack interface (e.g. a low-powered server). A weakness leads to an unwanted incident as derived in step 2 and requires a certain system knowledge as described below.
- Step 4.1 b: identification of attack method (threat agent):
  - A *threat agent* is an entity that can adversely act on assets. In the eTVRA model, the *threat agent* is a model element that models the behaviour of the attacker. *A threat agent* exploits a vulnerability through e.g. a vulnerability port and/or an attack interface.
  - The threat agent provides the attack vector. A threat is part of a certain threat family which threaten one of the security objectives identified from step 1.

When inserting a threat to the database the aim is to identify and allocate risk using the attack factors defined in TS 102 165-1 [i.1] combined with the value assigned as the impact of the loss of each asset.

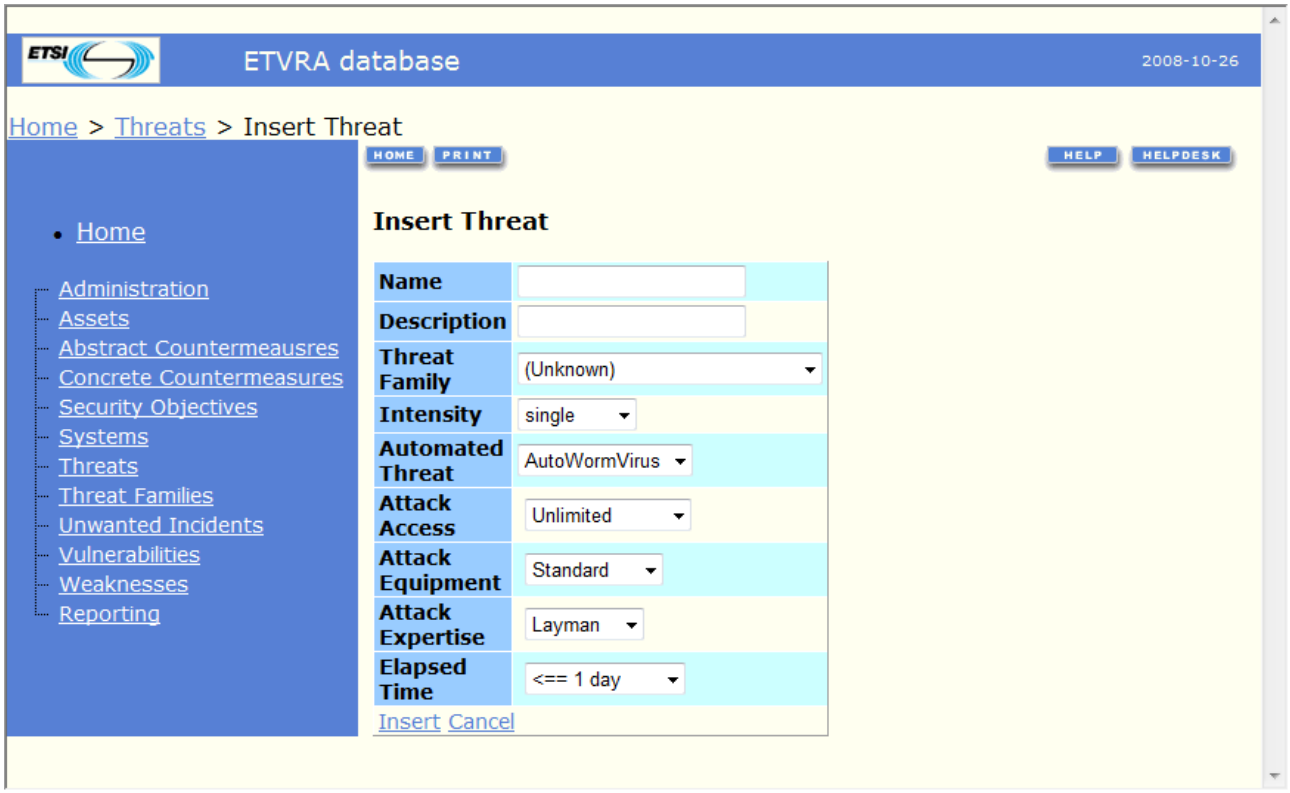


Figure 14: Screen shot for adding a threat

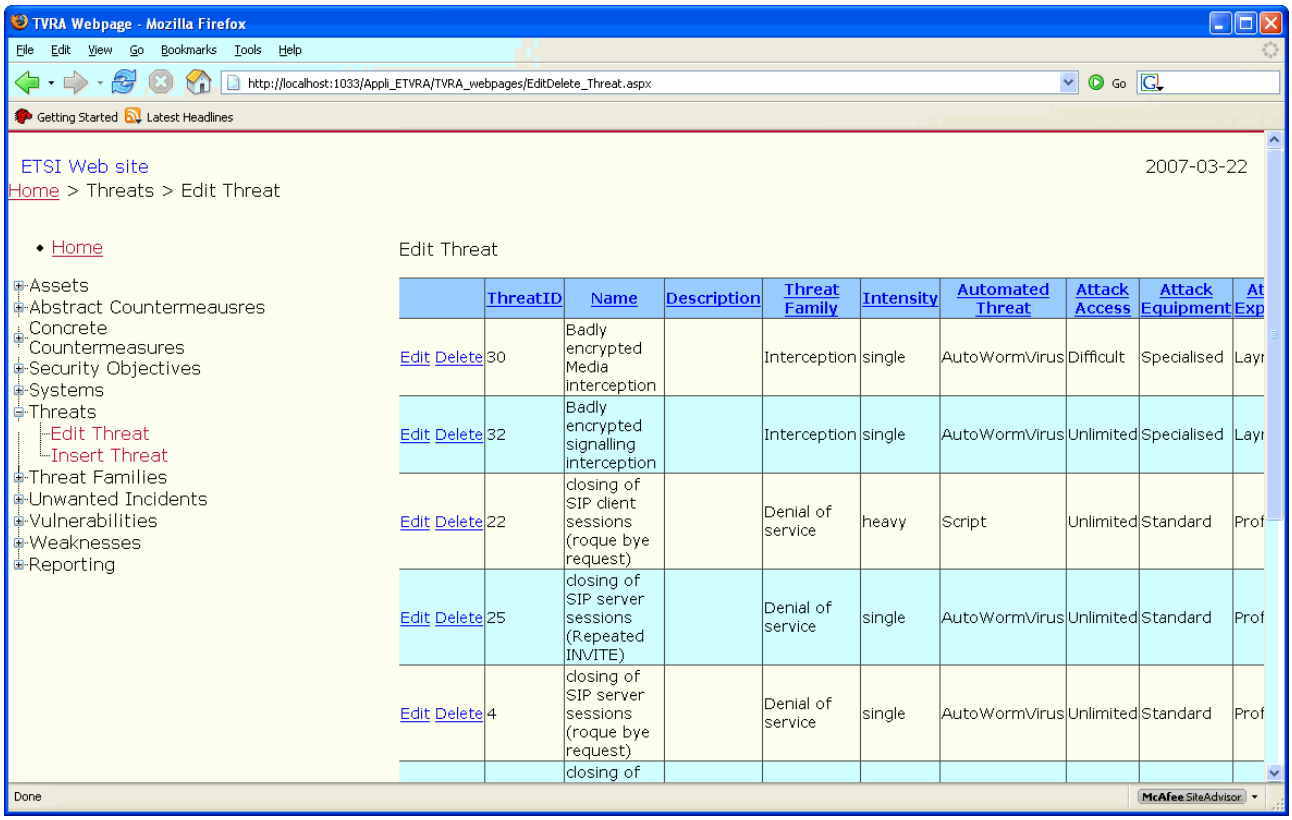


Figure 15: Screen shot for editing a threat

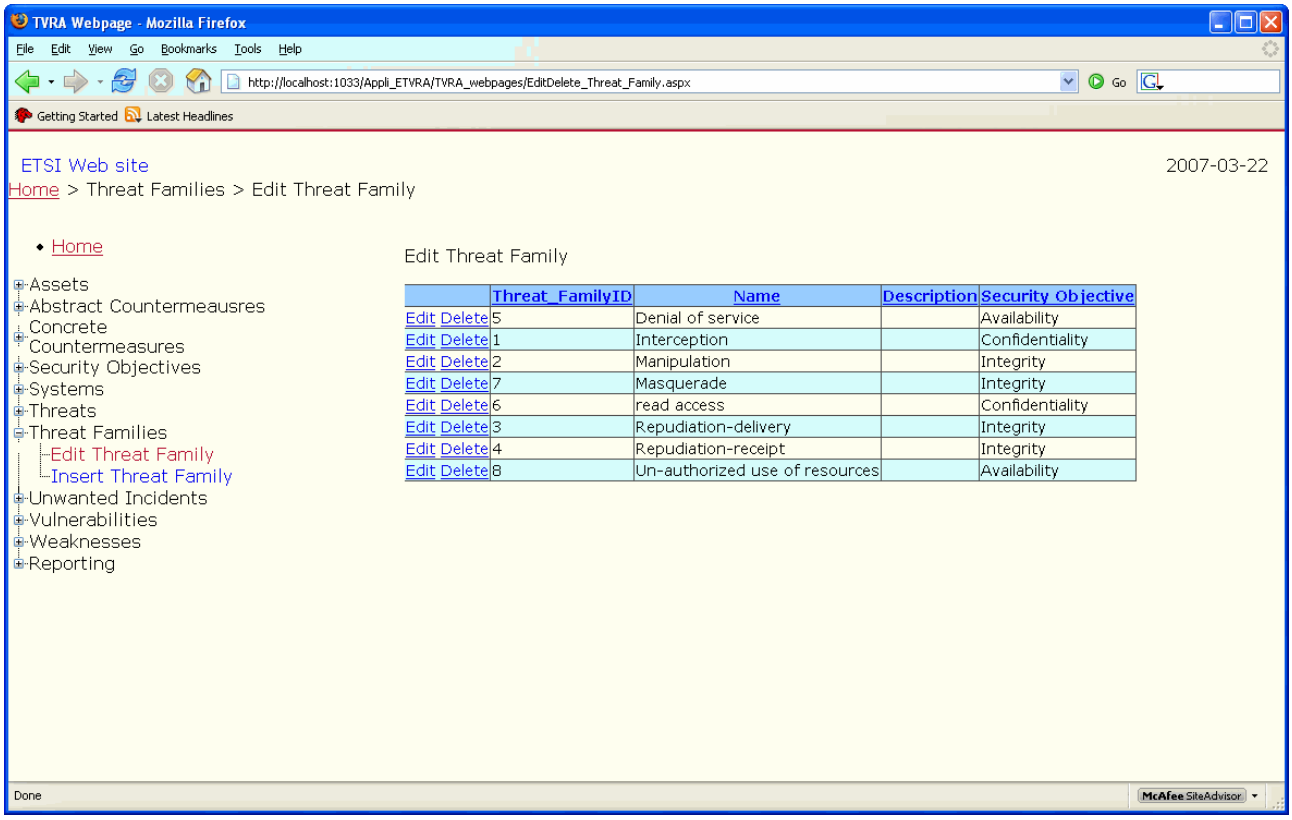


Figure 16: Screen shot for editing a threat family

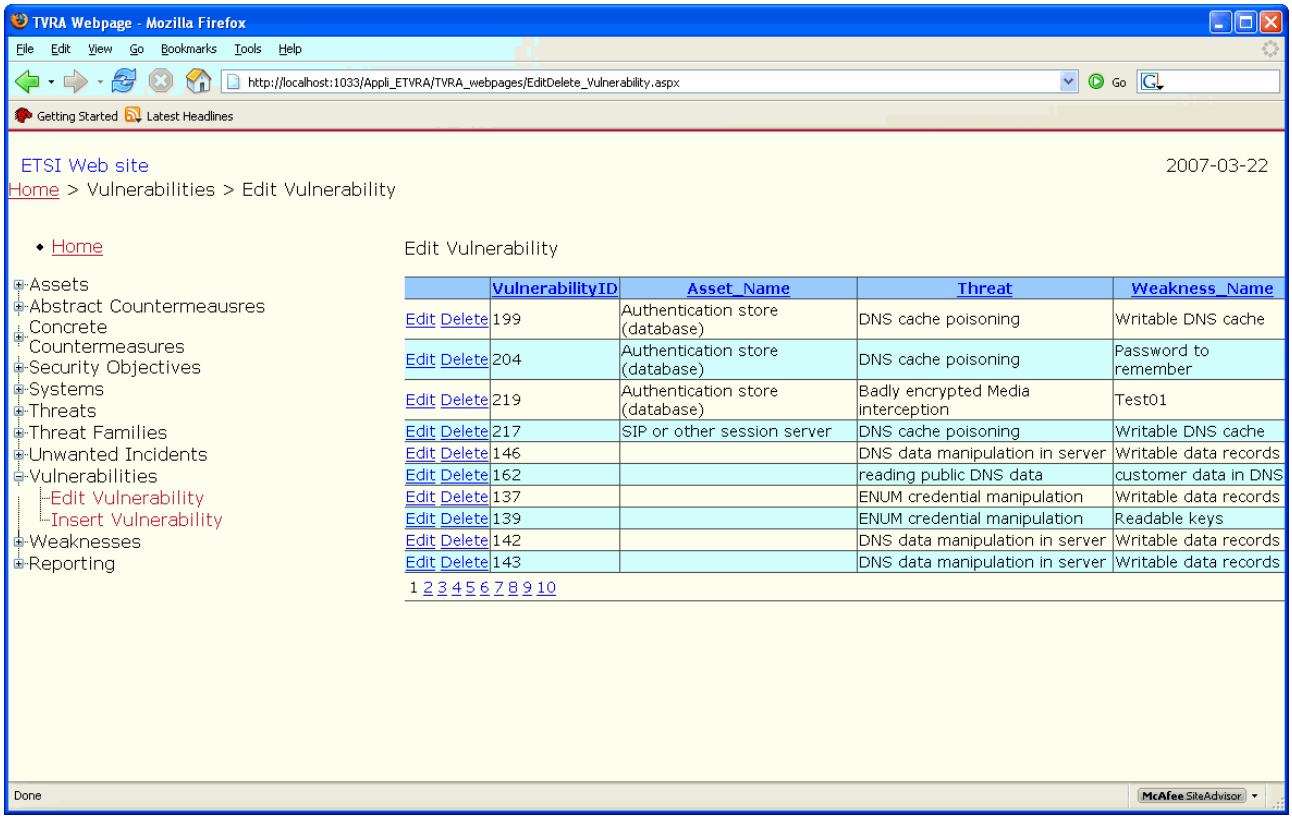


Figure 17: Screen shot for editing a vulnerability

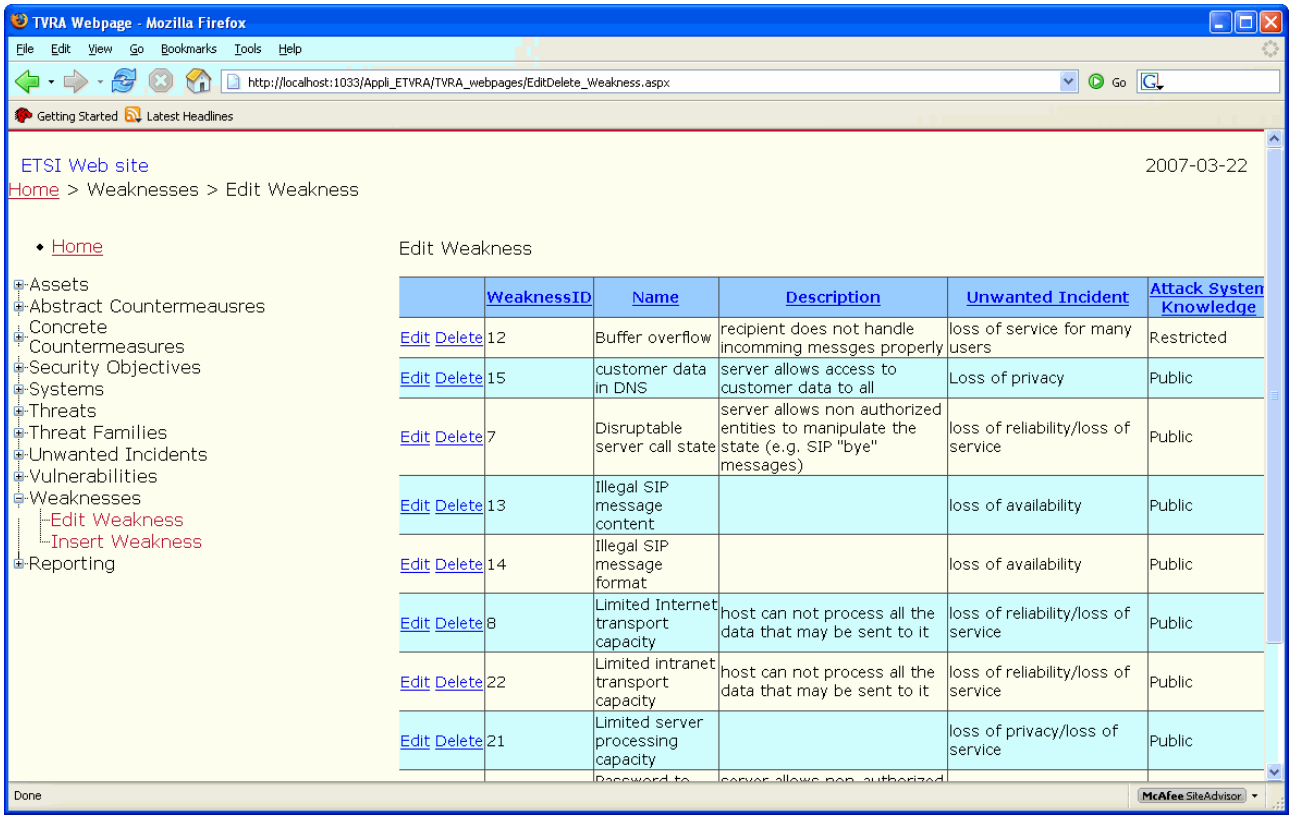


Figure 18: Screen shot for editing a weakness

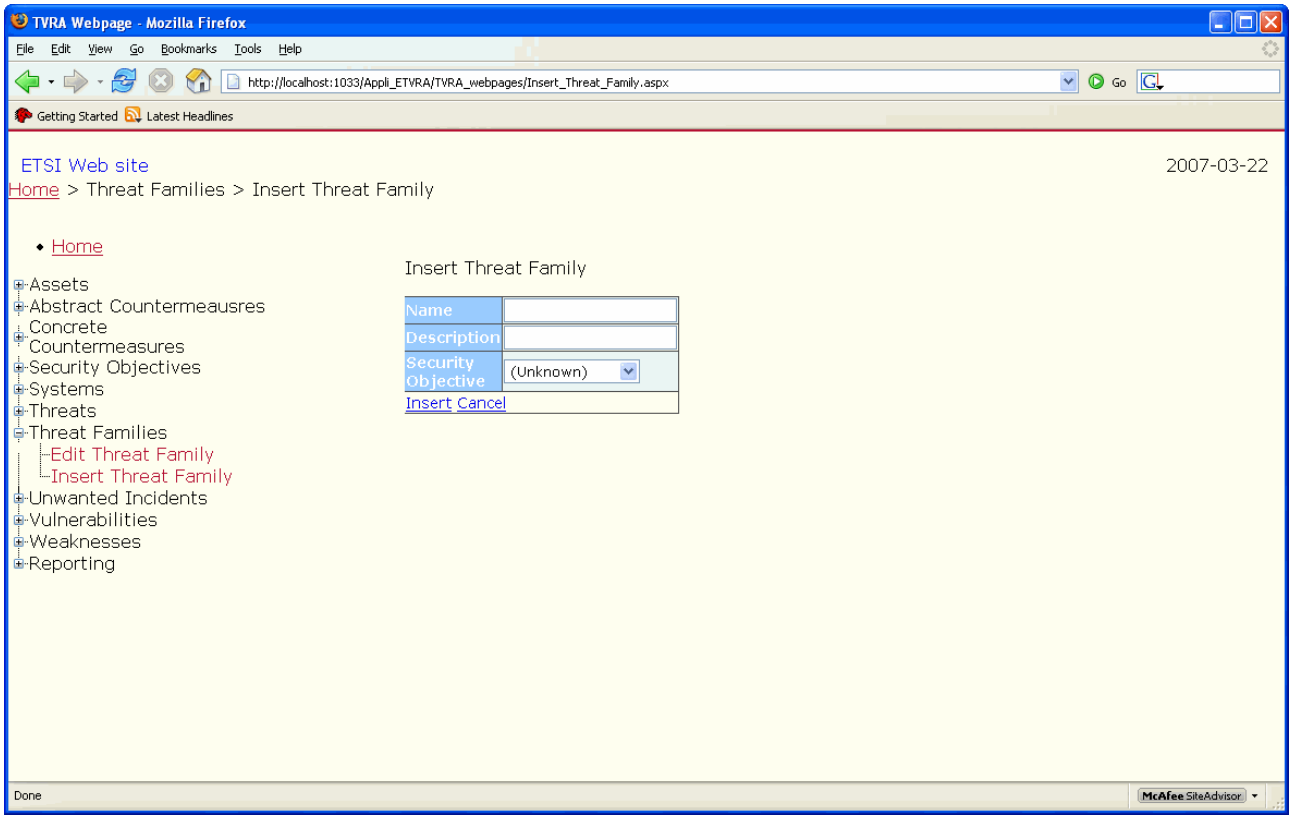


Figure 19: Screen shot for adding a threat family

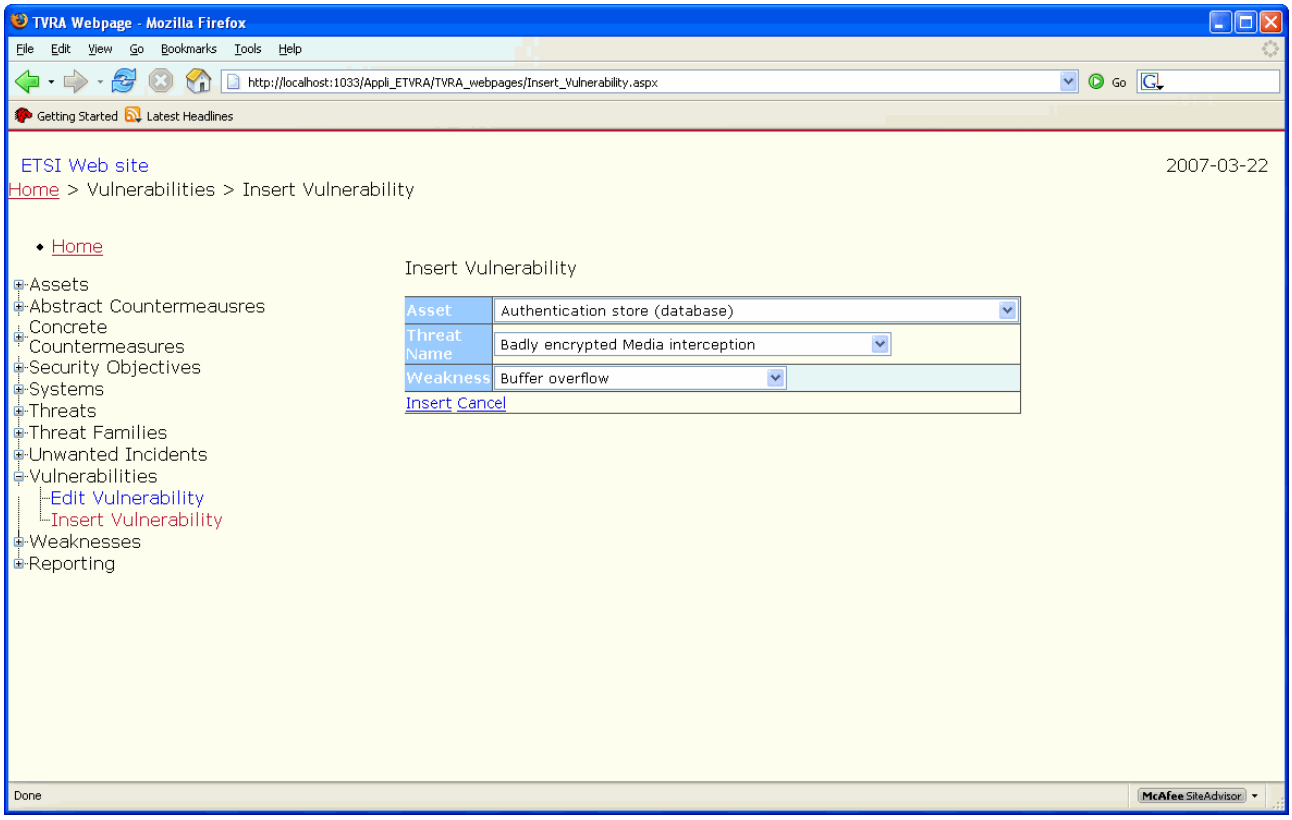


Figure 20: Screen shot for adding a vulnerability

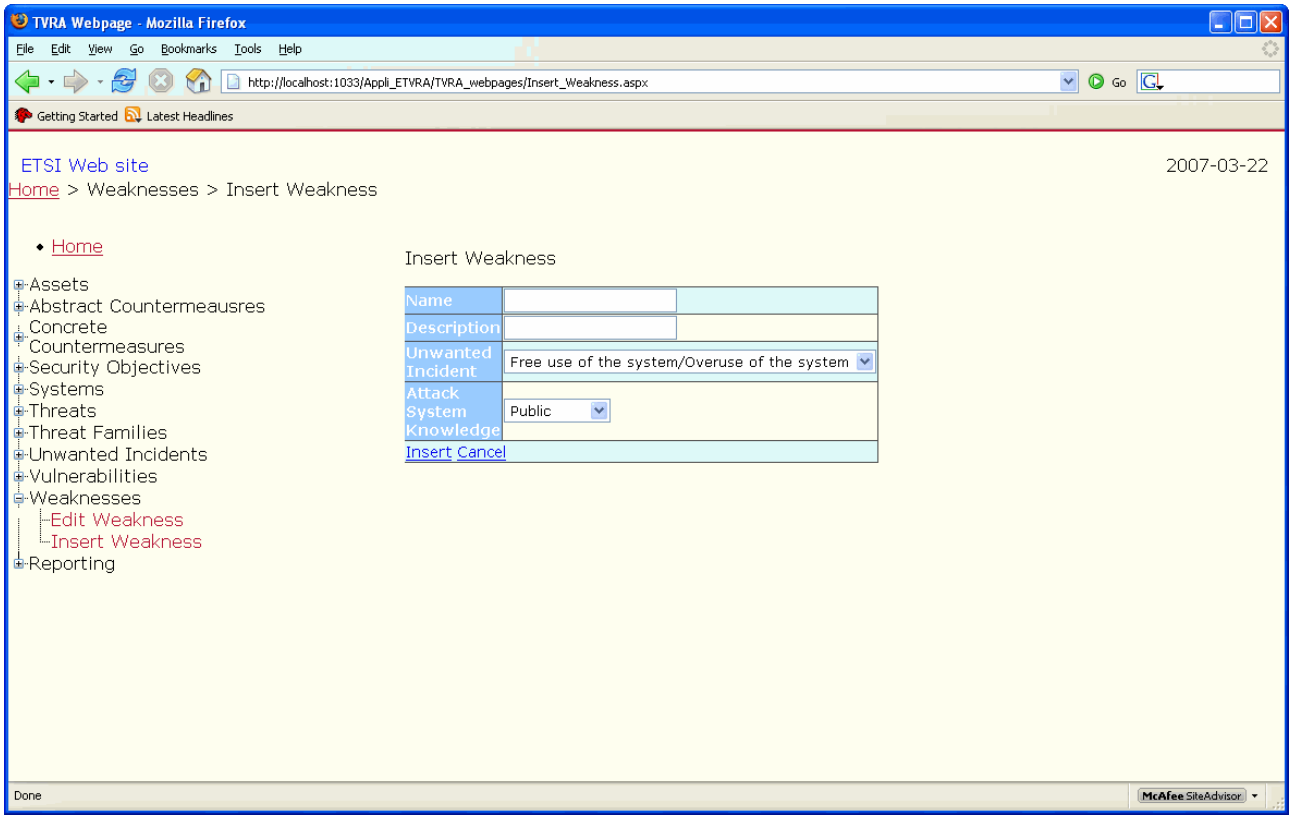


Figure 21: Screen shot for adding a weakness

5.6 Risk reporting

The eTVRA offers 2 standard reports:

- critical risks (i.e. only those with risk value of 6 or 9);
- all risks (i.e. all risk values).

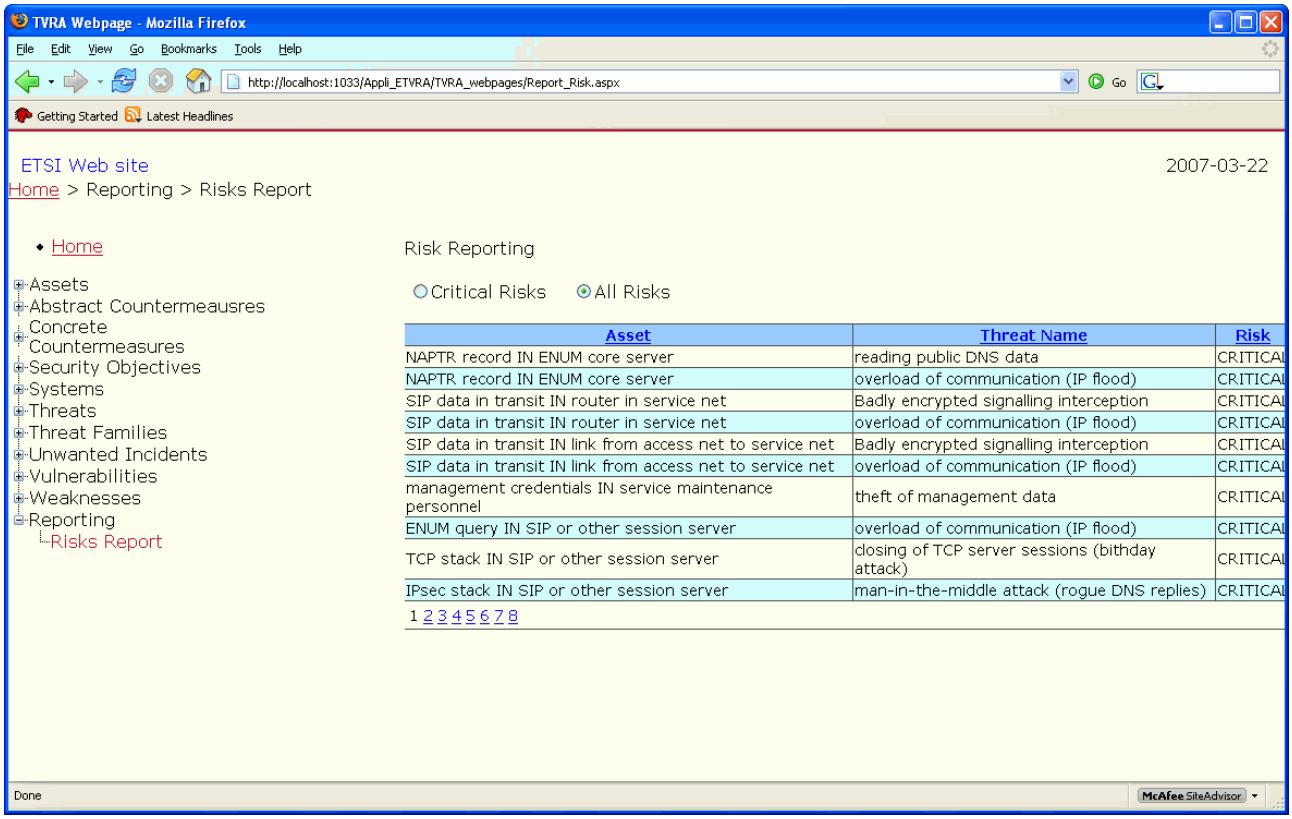


Figure 22: Screen shot of risk report (all risks)

History

Document history		
V2.1.1	February 2009	Publication