Certification Report

Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0388-2007

for

IBM Tivoli License Compliance Manager, Version 2.2, Fix Pack 1

from

IBM Corporation

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)3018 9582-0, Fax +49 (0)3018 9582-5455, Infoline +49 (0)3018 9582-111

Deutsches
IT-Sicherheitszertifikat

erteilt vom

Bundesamt für Sicherheit in der Informationstechnik

BSI

Bundesamt für Sicherheit
in der Informationstechnik

BSI-DSZ-CC-0388-2007

IBM Tivoli License Compliance Manager, Version 2.2, Fix Pack 1

from

IBM Corporation

Common Criteria Arrangement

The IT product identified in this certificate has been evaluated at an accredited and licensed/ approved evaluation facility using the *Common Methodology for IT Security Evaluation, Version 2.3* (ISO/IEC 15408:2005) for conformance to the *Common Criteria for IT Security Evaluation, Version 2.3 (ISO/IEC 15408:2005)*.

Evaluation Results:

Functionality:	**Product specific Security Target** **Common Criteria Part 2 extended**
Assurance Package:	**Common Criteria Part 3 conformant** **EAL2 augmented by ALC_FLR.1 - Basic Flaw remediation**

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

The notes mentioned on the reverse side are part of this certificate.

Bonn, 14th February 2007

The President of the Federal Office
for Information Security

IT Security Certified

SOGIS - MRA

Dr. Helmbrecht L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 228 9582-0 - Fax +49 228 9582-5455 - Infoline +49 228 9582-111

The rating of the strength of functions does not include the cryptoalgorithms suitable for encryption and decryption (see BSIG Section 4, Para. 3, Clause 2).

This certificate is not an endorsement of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

Contents

A Certification

1 Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125)
- Common Criteria for IT Security Evaluation (CC), version 2.3[5]
- Common Methodology for IT Security Evaluation (CEM), version 2.3
- BSI certification: Application Notes and Interpretation of the Scheme (AIS)

---

2 Act setting up the Federal Office for Information Security (BSI-Errichtungsgesetz, BSIG) of 17 December 1990, Bundesgesetzblatt I p. 2834

3 Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 7 July 1992, Bundesgesetzblatt I p. 1230

4 Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

5 Proclamation of the Bundesministerium des Innern of 10 May 2006 in the Bundesanzeiger dated 19 May 2006, p. 3730

2 Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1 ITSEC/CC - Certificates

The SOGIS-Agreement on the mutual recognition of certificates based on ITSEC became effective on 3 March 1998. This agreement was signed by the national bodies of Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland and the United Kingdom. This agreement on the mutual recognition of IT security certificates was extended to include certificates based on the CC for all evaluation levels (EAL 1 – EAL 7).

2.2 CC - Certificates

An arrangement (Common Criteria Arrangement) on the mutual recognition of certificates based on the CC evaluation assurance levels up to and including EAL 4 was signed in May 2000. It includes also the recognition of Protection Profiles based on the CC. The arrangement was signed by the national bodies of Australia, Canada, Finland, France, Germany, Greece, Italy, The Netherlands, New Zealand, Norway, Spain, United Kingdom and the United States. Israel joined the arrangement in November 2000, Sweden in February 2002, Austria in November 2002, Hungary and Turkey in September 2003, Japan in November 2003, the Czech Republic in September 2004, the Republic of Singapore in March 2005, India in April 2005.

3 Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product IBM Tivoli License Compliance Manager, Version 2.2, Fix Pack 1 has undergone the certification procedure at BSI.

The evaluation of the product IBM Tivoli License Compliance Manager, Version 2.2, Fix Pack 1 was conducted by atsec information security GmbH. The atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by BSI.

The sponsor, vendor and distributor is:

IBM Corporation
Via Sciangai, 53
Roma 00144, Italia

The certification is concluded with

- the comparability check and
- the production of this Certification Report.

This work was completed by the BSI on 14th February 2007.

The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, where specified in the following report.

This Certification Report only applies to the version of the product indicated here. The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

For the meaning of the assurance levels and the confirmed strength of functions, please refer to the excerpts from the criteria at the end of the Certification Report.

[6] Information Technology Security Evaluation Facility

4 Publication

The following Certification Results contain pages B-1 to B-22.

The product IBM Tivoli License Compliance Manager, Version 2.2, Fix Pack 1 has been included in the BSI list of the certified products, which is published regularly (see also Internet: http:// www.bsi.bund.de). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the vendor[7] of the product. The Certification Report can also be downloaded from the above-mentioned website.

[7] IBM Corporation
Via Sciangai, 53
Roma 00144, Italia

B Certification Results

The following results represent a summary of

- the security target of the sponsor for the target of evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

Contents of the certification results

1 Executive Summary

IBM Tivoli License Compliance Manager, version 2.2, Fix Pack 1 (named TLCM in short) is a software only product that provides software inventory, use metering, and license allocation services. Information about installed software and software use (software usage records) is collected from monitored computers and stored in a central DB2 database that is part of the TOE environment. The software usage records can be accessed by an authorized administrator to produce reports for billing and tracking of software license use within a defined organization.

Tivoli License Compliance Manager is based on a three-tier architecture composed of multiple servers with associated databases, agents, and related components supporting the product's functionality. The **Administration Server**, the **Runtime Server(s)** and **Agents** are considered to be the TOE. The databases and other supporting components are located in the TOE environment. For more details about the architectural description of the product, please refer to chapter 5 of this report.

Tivoli License Compliance Manager is an internally-deployed system, accessible only by a trusted and competent group of administrators in a controlled environment. There are no typical "end users" interacting with the product.

The TOE provides the following security functionality:

- Identification and authentication with password policy enforcement
- Session timeout
- Security Roles
- Management of Roles and Security Functions
- Secure data transfer between components
- Guaranteed data delivery

The product is available in two forms:

- A full commercial form that enables enterprise-wide monitoring and management of both IBM and non-IBM software products, including software products defined by an authorized administrator.
- A subset form that tracks installation and use of specific IBM software products to enable reporting requirements associated with the sub-capacity pricing model.

The security functions are the same for both forms of the product.

The IT product IBM Tivoli License Compliance Manager, Version 2.2, Fix Pack 1 was evaluated by atsec information security GmbH. The evaluation was completed on 25 January 2007. The atsec information security GmbH is an evaluation facility (ITSEF)[8] recognised by BSI.

The sponsor, vendor and distributor is

IBM Corporation
Via Sciangai, 53
Roma 00144, Italia

1.1 Assurance package

The TOE security assurance requirements are based entirely on the assurance components defined in part 3 of the Common Criteria (see Annex C or [1], part 3 for details). The TOE meets the assurance requirements of assurance level EAL2 (Evaluation Assurance Level 2 augmented by ALC_FLR.1). The following table shows the augmented assurance components.

Requirement	**Identifier**
EAL2	TOE evaluation: structurally tested
+: ALC_FLR.1	Life-cycle – Basic flaw remediation

Table 1: Assurance components and EAL-augmentation

1.2 Functionality

The TOE Security Functional Requirements (SFR) selected in the Security Target are Common Criteria Part 2 extended as shown in the following tables.

The following SFRs are taken from CC part 2:

Security Functional Requirement	**Addressed issue**
FDP	**User data protection**
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based control
FDP_ITT.1	Basic internal transfer protection
FIA	**Identification and authentication**
FIA_ATD.1	User attribute definition
FIA_SOS.1	Verification of secrets
FIA_UAU.2	User authentication before any action

[8] Information Technology Security Evaluation Facility

Security Functional Requirement	Addressed issue
FIA_UID.2	User identification before any action
FMT	**Security Management**
FMT_MOF.1	Management of security functions behavior
FMT_MSA.3	Static attribute initialization
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security management roles
FTA	**TOE Access**
FTA_SSL.3	TSF-initiated termination

Table 2: SFRs for the TOE taken from CC Part 2

The following CC part 2 extended SFRs are defined:

Security Functional Requirement	Addressed issue
FMT	**Security Management**
FMT_MSA.1a	Management of security attributes (Super Administrator)
FMT_MSA.1b	Management of security attributes (user)

Table 3: SFRs for the TOE, CC part 2 extended

Note: Only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST chapter 5.1.

The following Security Functional Requirements are defined for the IT-Environment of the TOE:

Security Functional Requirement	Addressed issue
FPT	**Protection of the TSF**
FPT_STM.1	Reliable time stamps

Table 4: SFRs for the IT-Environment

Note: Only the titles of the Security Functional Requirements are provided. For more details and application notes please refer to the ST chapter 5.3.

These Security Functional Requirements are implemented by the TOE Security Functions:

TOE Security Function	Addressed issue
SF.IA	Identification and Authentication
SF.IA.1	User to Administration Server identification and authentication
SF.IA.2	Password policy enforcement
SF.IA.3	Agent to Runtime Server identification and authentication

TOE Security Function	Addressed issue
SF.IA.4	Runtime Server to Administration Server identification and authentication
SF.IA.5	Inactivity timeout
SF.ACCESS	Access Control
SF.DATA	Data Protection During Transfer
SF.DATA.1	Agent to Runtime Server secure channel
SF.DATA.2	Data availability protection
SF.MGMT	Management of Security Functions
SF.MGMT.1	Create and manage organizations
SF.MGMT.2	Create and manage users
SF.MGMT.3	Change own user passwords
SF.MGMT.4	Change Runtime Server communication password
SF.MGMT.6	Change the Runtime Server Database password
SF.MGMT.7	Change the password used to open the truststore file
SF.MGMT.8	Re-encrypt all passwords
SF.MGMT.9	Change the Administration Server Database password
SF.MGMT.10	Re-encrypt all passwords
SF.MGMT.11	Define and manage runtime server security attributes

Table 5: Security Functions

For more details please refer to the Security Target [6], chapter 6.1

1.3 Strength of Function

The TOE's strength of functions is claimed basic (SOF-basic) for specific functions as indicated in the Security Target [6], chapter 8.3.3.

1.4 Summary of threats and Organisational Security Policies (OSPs) addressed by the evaluated IT product

The Security Target [6] describes the threats to be countered by the TOE and its environment in terms of human threat agents and assets potentially subject to attacks.

The only asset described is the following:

- **Software Usage Records**: Software installation and use data collected by the Agents deployed on monitored computers, transmitted through the Runtime Server and the Administration Server, and stored in an external Administration Server DB2 database.

The threat agents, their attack potential, resources, and level of expertise are described below:

- **User**: This threat agent is a legitimate human user in the TOE environment. Non-administrator TOE users have no authorized access at all to the TOE resources, but may attempt to access assets protected by the system. This threat agent is considered to have a low motivation to attack, limited resources, and limited opportunity, but might have a high level of expertise and competence.
- **Non authorized administrator**: This threat agent is a legitimate human administrator of the TOE with access to specific data or function of TOE, but without authorized access to other data or function functions of TOE. An administrator with limited access might attempt to access assets he or she is not authorized to access. This threat agent is considered to have a low motivation to attack and limited resources, but has a high level of expertise, competence, and opportunity.

It is assumed that both sets of potential attackers come from a well-managed user community in a non-hostile working environment. The TOE is not intended to be used in an environment in which protection against determined or sophisticated attacks is required.

The following threats must be countered by security functions implemented by the TOE:

- **T.BYPASS**: A user or a non-authorized administrator might bypass TSP enforcement functions to access data or resources protected by the TOE by penetrating or manipulating portions of the TOE.
- **T.ACCESS**: An administrator might see software usage records for an organization in which he or she does not play a role.
- **T.DATA_INT**: A user or a non-authorized administrator might compromise the integrity or confidentiality of data being transferred from the Agent to the Runtime Server.

- **T.DATA_PERSIST**: A legitimate user (because of user error), an attacker (maliciously), or a system error might cause loss of data by interfering with successful completion of the transfer of data from one TOE component to another component (successful completion means successful write to the target database).

Please note that no organizational security policies for the TOE are described.

1.5 Special configuration requirements

The evaluated configuration of the IBM Tivoli License Compliance Manager, Version 2.2, Fix Pack 1 servers, can be used on the following range of operating system platforms:

- Windows Server 2003 Standard or Enterprise Edition,
  Windows 2000 Advanced Server or Windows 2000 Server
- IBM AIX 5.3 and 5.2
- HP/UX 11i
- Red Hat Enterprise Linux 4.0 and 3.0
- SUSE LINUX Enterprise Server 9 and 8
- Sun Solaris 10 and 9

The evaluated configuration of Tivoli License Compliance Manager Agents are allowed to be used on the following operating system platforms:

- Windows Server 2003 Standard Edition
- IBM AIX 5.3
- Sun Solaris 9
- Red Hat Enterprise Linux 4.0

Please consider the platforms on which the TOE testing has been carried out (refer to chapter 7).

The Agents include IBM Global Security Kit (GSKit) as part of the TOE. It is a library package that implements SSL. The following GSKit versions are used:

Supported Agent Operating System	**GSKit Version**
AIX	7.0.3.15
Linux	7.0.3.15
Sun Solaris	7.0.3.17
Windows	7.0.3.20

Table 6: Supported GSKit versions

The TOE can be purchased through established IBM product distribution channels. It may be acquired either by secure electronic download or by requesting and installing from physical media (CD-ROM or DVD).

In the evaluated configuration, the fix pack component of the TOE (Fix Pack 1) must be acquired and is only available on CD-ROM through an established IBM Tivoli support channel.

The following installation requirements are described in the ST [6]:

- The TOE must be configured to use the database authentication mechanism.
- The TOE must be configured to use SSL with client authentication to protect data flow between the Agents and the Runtime Server.
- The Runtime Server Agent Self Update feature must be disabled.

1.6 Assumptions about the operating environment

The following assumptions about the environment of the TOE are made:

- **A.PHYSICAL**: It is assumed that all machines housing components of the TOE and components in the TOE environment on which the TOE relies are protected against unauthorized physical access and modification.
- **A.TIME**: It is assumed that a reliable time function is provided by the TOE environment to support the inactivity timeout function.

1.7 Disclaimers

The Certification Results only apply to the version of the product indicated in the Certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2 Identification of the TOE

The Target of Evaluation (TOE) is called:

IBM Tivoli License Compliance Manager, Version 2.2, Fix Pack 1

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	IBM Tivoli License Manager	Version 2.2: PID number 5724-D33	CD-ROM or Download
2	SW	Fix Pack 1	part number 2.2.0-TIV-TLCM-FP0001	CD-ROM
3	DOC	ADMINGUIDE	SC32-1430-02	PDF
4	DOC	CATMGMT	SC32-1434-01	PDF
5	DOC	CCGUIDE	First Ed.	PDF
6	DOC	COMMANDREF	SC32-1501-00	PDF
7	DOC	DATADICT	SC32-1432-02	PDF
8	DOC	FPREADME	First Ed.	PDF
9	DOC	INSTALL	SC32-1431-02	PDF
10	DOC	OVERVIEW	SC32-1503-00	PDF
11	DOC	PROBDETER	SC32-9102-01	PDF
12	DOC	RELNOTES	SC32-1429-02	PDF
13	DOC	SECMGMT	SC32-1502-00	PDF

Table 7: Deliverables of the TOE

The following licensed program packages that delivered together with the TOE. They have to be installed as prerequisites for the TOE as part of the TOE environment:

- IBM WebSphere Application Server (WAS) version 6.0
- IBM WebSphere Application Server plug-in, version 6.0
- IBM HTTP Web server, version 6.0
- IBM DB2 Universal Database, Enterprise Edition, version 8.2

Please note that the TOE component GSKit in the versions as listed in chapter 1.5 of this report is also delivered with the TOE.

No hardware is delivered as part of the product.

3 Security Policy

IBM Tivoli License Compliance Manager, version 2.2, Fix Pack 1 provides software inventory, use metering and license allocation services.

Therefore its main purpose is to provide mechanisms for Authentication and to control the access to protected ressources. As the TOE consists of more than one component, protection of data transfer between the components is implemented. Management functionality is provided to support these functionalities.

The Security Policy of the TOE is defined by the following TOE security functional requirements:

- SFR components of the class FIA define the mechanisms for identification and authentication
- SFR components of the class FDP define the access control for protected ressources and the protection of data transfer between the components of the TOE
- SFR components of the class FMT define the management functions that the TOE provides

A detailed description/definition of the Security Policy enforced by the TOE is given in the Security Target [6], chapter 5.1 by the definition of the TOE Security Functional Requirements.

4 Assumptions and Clarification of Scope

The security aspects of the environment in which the TOE is expected to be used are described in terms of assumptions. The assumptions for the environment are divided into assumptions about the intended usage of the TOE and assumptions about the environment the TOE is going to be used in.

4.1 Usage assumptions

- **A.CRYPTO**: It is assumed that cryptographic keys and certificates used in authentication between components of the TOE are generated, managed, and stored in a secure way to ensure their confidentiality and integrity.
- **A.ENV_CONFIG**: It is assumed that the TOE environment is configured and well managed in accordance with the administrator documentation to protect the TOE and its data, including when data is transferring from the Runtime Server to the Administration Server and when data is transferring between each server and its associated database.
- **A.TOE_CONFIG**: It is assumed that the TOE is configured and operated in accordance with the administrator documentation and that the Agent software is installed using a secure deployment method for the intended environment as documented in the administrator documentation.
- **A. DATA_INT**: It is assumed that administrators will ensure the integrity and confidentiality of data transferred between the Runtime Server and the Administration Server.

4.2 Environmental assumptions

- **A.PHYSICAL**: It is assumed that all machines housing components of the TOE and components in the TOE environment on which the TOE relies are protected against unauthorized physical access and modification.
- **A.TIME**: It is assumed that a reliable time function is provided by the TOE environment to support the inactivity timeout function.
- **A.TOE_ADMIN**: It is assumed that TOE Administrators are competent and trustworthy to perform their tasks, and that organizational procedures and policies are sufficient to ensure that they are held accountable for their security-relevant actions.
- **A. ENV_ADMIN**: It is assumed that TOE Environment Administrators (e.g., individuals who have administrator privileges on the administration and runtime databases) are competent and trustworthy to perform their tasks.
- **A.COOP**: It is assumed that all non-administrator users in the environment are part of a well-managed and cooperative user community.

4.3 Clarification of scope

The threats described below must be countered by security means implemented by the TOE environment.

- **TE.PASS**: A user or a non-authorized administrator might bypass the TOE to access data or resources protected by the TOE by attacking the underlying operating system or database.
- **TE.SPOOF**: A user or a non-authorized administrator might record or modify user data on an inter-TOE communication link or on a communication link between TOE and non-TOE components in order to obtain unauthorized access to user data or to manipulate user data to be recorded.

5 Architectural Information

Tivoli License Compliance Manager is based on a three-tier architecture composed of multiple servers with associated databases, Agents, and related components supporting the product's functionality. Figure 1 shows a simple deployment.

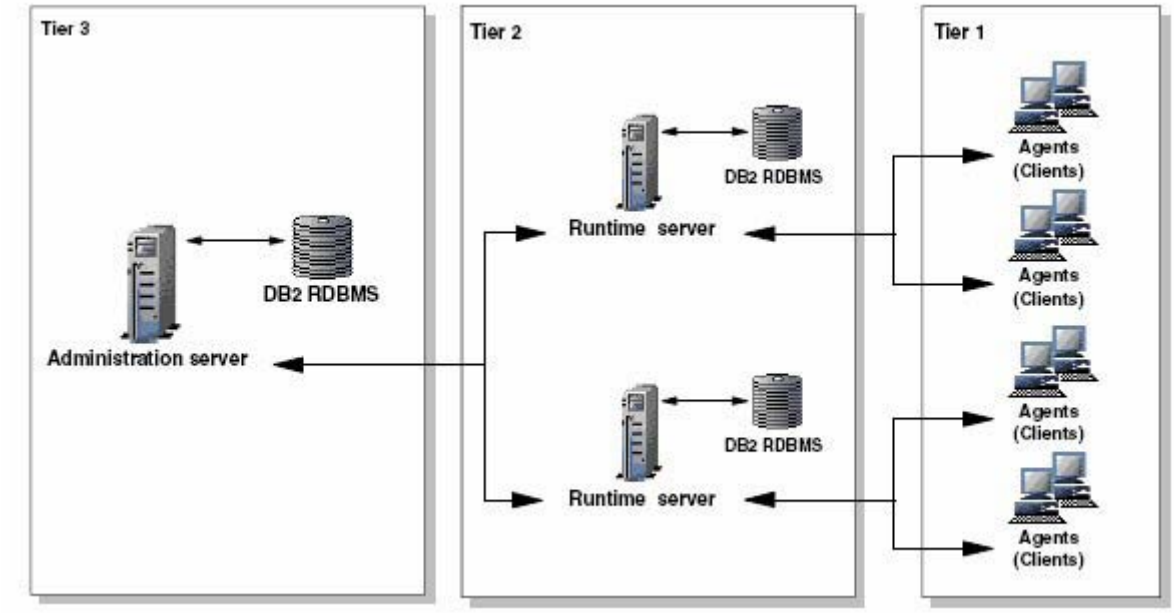

Figure 1: Three-tier architecture of the TOE

These are the main components of Tivoli License Compliance Manager, as illustrated in Figure 1:

- A single Administration Server through which various administrative, monitoring, and reporting capabilities are provided and which with its associated DB2 database, provides a repository for product, license agreement, license use, installed software, and organization information. (In the context of this evaluation, the DB2 database is part of the environment, not part of the TOE.)
- One or more Runtime Servers, which act as a proxy between Agents and the Administration Server and supply information required by the Agents to support software monitoring tasks. Each Runtime Server has an associated DB2 database. Scalability of the monitored organization is addressed by adding more Runtime Servers as needed in order to balance performance requirements. (In the context of this evaluation, the DB2 database is part of the environment, not part of the TOE.)
- A license management Agent deployed on each computer that is to be monitored. The Agent performs an inventory of the software installed on the computer and monitors use of installed software products, and forwards this information (software usage records) to the Runtime Server, which in turn forwards the software usage records to the Administration Server.

As shown in Figure 1, the software usage records managed by the TOE flow from the Agents to the Runtime Servers, then from the Runtime Servers to the Administration Server.

The hierarchical structure of Tivoli License Compliance Manager allows for flexible deployment. For example, the Administration Server and Runtime Server components can be deployed on the same machine, or Runtime Servers may be deployed within the same physical network as the Administration Server, or Runtime Servers may be deployed at remote locations. Agents may be deployed on machines physically within or outside the secure network. Administrators are trusted to make appropriate decisions to ensure secure communication if components are not deployed within a secure network.

6 Documentation

For a listing of the documentation delivered with the TOE please refer to chapter 2 or chapter 14 (documents [8] to [18]) of this report.

7 IT Product Testing

7.1 Developer Testing

Testing approach

A test plan is used by the testing personnel to set-up the test environment. The tests have been performed in the IBM test lab at the Rome facility. The test cases are performed manually using the GUI interface and the command-line. They are fully described in the test plan.

Tests that have been performed for the evaluated version are recorded in a test tracking tool based on a Lotus Notes database. The test records the number of times a test has been performed and the results (pass or fail) for each run.

Testing configuration

Testing of the server components is performed on a Solaris System which is used for both the runtime and the admin server. The test environment was set up in the IBM Rome test lab according to the instructions in the test plan which is compliant with the evaluated configuration. As the server components of the TOE rely on an underlying Java layer as the abstract machine (which is part of the environment and is provided with the IBM WebSphere Application Server 6.0) there is no dependency on the real hardware.

The server software used for testing was installed from CDs or a central repository where the contents of the CDs have been copied to. The server software used for testing was IBM Tivoli License Compliance Manager, Version 2.2, Fix Pack 1.

The clients (systems the TLCM Agent is running on) used for testing used the following operating systems as listed in the Security Target:

- Sun Solaris 9
- Windows Server 2003 Standard Edition
- IBM AIX 5.3
- Red Hat Enterprise Linux 4.0

The GSKit Versions used were:

- AIX: GSKit Version 7.0.3.15
- Linux: GSKit Version 7.0.3.15
- Solaris: GSKit Version 7.0.3.17
- Windows: GSKit Version 7.0.3.20

The underlying/supporting software of the TOE environment for the test was:

- IBM WebSphere Application Server 6.0
- IBM WebSphere Application Server plug-in 6.0
- IBM HTTP Web Server 6.0
- IBM DB2 Universal Database, Enterprise Edition 8.2

Test results

Test results are recoded as pass / fail counters in a test tracking tool (a Notes database). All tests where recorded as pass for each iteration performed.

Test coverage and depth

The developer provided a test coverage analysis where test cases are mapped to FSP/TSFI and SF. It shows a full coverage of all TSF and TSFI.

Conclusion

Developer testing was performed in an ST conformant TOE environment with a TOE in a version and configuration also in line with the ST.

The developers test coverage and the depth of the testing was analysed by reviewing all test cases in the test plan. The evaluator found the testing of the TSF to be sufficient and covering the TSF as identified in the functional specification.

Test results provided by the developer have been found to be consistent with the test plan (i.e. all actual test results were as expected).

7.2 Evaluator Testing

TOE test configuration

The evaluator used the developers test environment in the lab in Rome. The systems (Server and Agents) were installed from install programs on a central file server. The install programs were verified against the shipped CD via MD5 checksums. The installation was performed in accordance with the “Common Criteria Secure Implementation and Configuration Guide” following the setup instructions in the developers test plan.

The same test set up and configuration as for the developer testing was used.

Chosen subset size

The evaluator chose to perform all of the CC specific tests of the developer.

Evaluator tests performed

In addition to the repetition of the developer tests the evaluator devised a set of own tests. These evaluator tests were not functional tests but penetration testing to augment the functional developer testing. The evaluator performed tests e.g. in the following areas:

- Vulnerability Scanning
- URL based penetration testing

Summary of Evaluator tests

The evaluator could perform the developer tests successfully with the provided test documentation. The evaluator tests confirmed the developer tests and extended the testing of the developer.

All tests have been successfully executed and produced the expected results.

8 Evaluated Configuration

The evaluated version of the TOE is IBM Tivoli License Compliance Manager, Version 2.2, Fix Pack 1 as described in the ST. This includes the following GSKit version for the different platforms the TOE can run on:

- AIX: GSKit Version 7.0.3.15
- Linux: GSKit Version 7.0.3.15
- Solaris: GSKit Version 7.0.3.17
- Windows: GSKit Version 7.0.3.20

The TOE has to be set-up in accordance to the guidance documentation [8] to [18] and the Security Target [6]

Both the developer and the evaluator have tested the server parts of the TOE on a Solaris System. The client part was tested on four different platforms:

- Sun Solaris 9
- Windows Server 2003 Standard Edition
- IBM AIX 5.3
- Red Hat Enterprise Linux 4.0

9 Results of the Evaluation

The Evaluation Technical Report (ETR), [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The evaluation methodology CEM [2] was used for those components identical with EAL2.

The verdicts for the CC, Part 3 assurance components (according to EAL2 augmented by SLC_FLR.1 and the class ASE for the Security Target evaluation) are summarised in the following table.

Assurance classes and components		**Verdict**
Security Target evaluation	CC Class ASE	PASS
TOE description	ASE_DES.1	PASS
Security environment	ASE_ENV.1	PASS
ST introduction	ASE_INT.1	PASS
Security objectives	ASE_OBJ.1	PASS
PP claims	ASE_PPC.1	PASS
IT security requirements	ASE_REQ.1	PASS
Explicitly stated IT security requirements	ASE_SRE.1	PASS
TOE summary specification	ASE_TSS.1	PASS
Configuration management	CC Class ACM	PASS
Configuration items	ACM_CAP.2	PASS
Delivery and operation	CC Class ADO	PASS
Delivery procedures	ADO_DEL.1	PASS
Installation, generation, and start-up procedures	ADO_IGS.1	PASS
Development	CC Class ADV	PASS
Informal functional specification	ADV_FSP.1	PASS
Descriptive high-level design	ADV_HLD.1	PASS
Informal correspondence demonstration	ADV_RCR.1	PASS
Guidance documents	CC Class AGD	PASS
Administrator guidance	AGD_ADM.1	PASS
User guidance	AGD_USR.1	PASS
Life cycle support	CC Class ALC	PASS
Basic flaw remediation	ALC_FLR.1	PASS
Tests	CC Class ATE	PASS

Assurance classes and components		Verdict
Evidence of coverage	ATE_COV.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing – sample	ATE_IND.2	PASS
Vulnerability assessment	CC Class AVA	PASS
Strength of TOE security function evaluation	AVA_SOF.1	PASS
Developer vulnerability analysis	AVA_VLA.1	PASS

Table 8: Verdicts for the assurance components

The evaluation has shown that:

- Security Functional Requirements specified for the TOE are Common Criteria Part 2 extended
- the assurance of the TOE is Common Criteria Part 3 conformant, EAL2 augmented by ALC_FLR.1.

The following TOE Security Functions fulfil the claimed Strength of Function:

- SF.IA.2 Password policy enforcement

The results of the evaluation are only applicable to the “IBM Tivoli License Compliance Manager,Version 2.2, Fix Pack 1” as described in chapter 2 of this report.

The validity can be extended to new versions and releases of the product, provided the sponsor applies for re-certification or assurance continuity of the modified product, in accordance with the procedural requirements, and the evaluation of the modified product does not reveal any security deficiencies.

10 Comments/Recommendations

The guidance documents [8] to [18] and the Security Target [6] contain necessary information about the usage of the TOE and all security hints therein have to be considered.

11 Annexes

None.

12 Security Target

For the purpose of publishing, the security target [6] of the target of evaluation (TOE) is provided within a separate document.

13 Definitions

13.1 Acronyms

BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
CC	Common Criteria for IT Security Evaluation
EAL	Evaluation Assurance Level
IT	Information Technology
PP	Protection Profile
SF	Security Function
SFP	Security Function Policy
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

13.2 Glossary

Augmentation - The addition of one or more assurance component(s) from CC Part 3 to an EAL or assurance package.

Extension - The addition to an ST or PP of functional requirements not contained in part 2 and/or assurance requirements not contained in part 3 of the CC.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - An entity within the TSC that contains or receives information and upon which subjects perform operations.

Protection Profile - An implementation-independent set of security requirements for a category of TOEs that meet specific consumer needs.

Security Function - A part or parts of the TOE that have to be relied upon for enforcing a closely related subset of the rules from the TSP.

Security Target - A set of security requirements and specifications to be used as the basis for evaluation of an identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Strength of Function - A qualification of a TOE security function expressing the minimum efforts assumed necessary to defeat its expected security behaviour by directly attacking its underlying security mechanisms.

SOF-basic - A level of the TOE strength of function where analysis shows that the function provides adequate protection against casual breach of TOE security by attackers possessing a low attack potential.

SOF-medium - A level of the TOE strength of function where analysis shows that the function provides adequate protection against straightforward or intentional breach of TOE security by attackers possessing a moderate attack potential.

SOF-high - A level of the TOE strength of function where analysis shows that the function provides adequate protection against deliberately planned or organised breach of TOE security by attackers possessing a high attack potential.

Subject - An entity within the TSC that causes operations to be performed.

Target of Evaluation - An IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

TOE Security Functions - A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.

TOE Security Policy - A set of rules that regulate how assets are managed, protected and distributed within a TOE.

TSF Scope of Control - The set of interactions that can occur with or within a TOE and are subject to the rules of the TSP.

14 Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 2.3, August 2005

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 2.3, August 2005

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE.

[5] German IT Security Certificates (BSI 7148, BSI 7149), periodically updated list published also on the BSI Web-site

[6] Security Target BSI-DSZ-0388-2007, Version 2.2, 18 December 2006 , Security Target for IBM Tivoli License Compliance Manager version 2.2, Fix Pack 1, IBM Italia s.p.a., Tivoli

[7] Evaluation Technical Report, Version 4, atsec information security GmbH, 24 January 2007, confidential document

User Guidance Documentation

[8] ITLM version 2.2 Administration, tlmadmst.pdf, SC32-1430-02, Feb 2006

[9] ITLM version 2.2 Catalog Management, tlmcmmst.pdf, SC32-1434-01, Feb 2006

[10] IBM Tivoli License Compliance Manager Version 2.2 Fix Pack 1 Common Criteria Secure Implementation and Configuration Guide, ITLCM 2.2 FP1 - CCGuide.pdf, First Ed., Sep 2006

[11] ITLM version 2.2 Commands, tlmcmdmst.pdf, SC32-1501-00, Feb 2006

[12] ITLM version 2.2 Data Dictionary, tlmddmst.pdf, SC32-1432-02, Feb 2006

[13] Readme File for Fix Pack 2.2.0 2013TIVTLCM-FP0001, FixPack1_readme.pdf, First Ed., 2006-06-01

[14] ITLM version 2.2 Planning, Installation, and Configuration, tlminmst.pdf, SC32-1431-02, Feb 2006

[15] ITLM version 2.2 Overview, tlmovmst.pdf, SC32-1503-00, Feb 2006

[16] ITLM version 2.2 Problem Determination, tlmpdmst.pdf, SC32-9102-01, Feb 2006

[17] ITLM version 2.2 Release Notes, tlmrnmst.pdf, SC32-1429-02, Feb 2006

[18] ITLM version 2.2 Security Management, tlmsmmst.pdf, SC32-1502-00, Feb 2006

C Excerpts from the Criteria

CC Part1:

Conformance results (chapter 7.4)

„The conformance result indicates the source of the collection of requirements that is met by a TOE or PP that passes its evaluation. This conformance result is presented with respect to CC Part 2 (functional requirements), CC Part 3 (assurance requirements) and, if applicable, to a pre-defined set of requirements (e.g., EAL, Protection Profile).

The conformance result consists of one of the following:

a) **CC Part 2 conformant** - A PP or TOE is CC Part 2 conformant if the functional requirements are based only upon functional components in CC Part 2.

b) **CC Part 2 extended** - A PP or TOE is CC Part 2 extended if the functional requirements include functional components not in CC Part 2.

plus one of the following:

a) **CC Part 3 conformant** - A PP or TOE is CC Part 3 conformant if the assurance requirements are based only upon assurance components in CC Part 3.

b) **CC Part 3 extended** - A PP or TOE is CC Part 3 extended if the assurance requirements include assurance requirements not in CC Part 3.

Additionally, the conformance result may include a statement made with respect to sets of defined requirements, in which case it consists of one of the following:

a) **Package name Conformant** - A PP or TOE is conformant to a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) include all components in the packages listed as part of the conformance result.

b) **Package name Augmented** - A PP or TOE is an augmentation of a pre-defined named functional and/or assurance package (e.g. EAL) if the requirements (functions or assurance) are a proper superset of all components in the packages listed as part of the conformance result.

Finally, the conformance result may also include a statement made with respect to Protection Profiles, in which case it includes the following:

a) **PP Conformant** - A TOE meets specific PP(s), which are listed as part of the conformance result.“

CC Part 3:

Assurance categorisation (chapter 7.5)

"The assurance classes, families, and the abbreviation for each family are shown in Table 1.

Assurance Class	Assurance Family
ACM: Configuration management	CM automation (ACM_AUT)
	CM capabilities (ACM_CAP)
	CM scope (ACM_SCP)
ADO: Delivery and operation	Delivery (ADO_DEL)
	Installation, generation and start-up (ADO_IGS)
ADV: Development	Functional specification (ADV_FSP)
	High-level design (ADV_HLD)
	Implementation representation (ADV_IMP)
	TSF internals (ADV_INT)
	Low-level design (ADV_LLD)
	Representation correspondence (ADV_RCR)
	Security policy modeling (ADV_SPM)
AGD: Guidance documents	Administrator guidance (AGD_ADM)
	User guidance (AGD_USR)
ALC: Life cycle support	Development security (ALC_DVS)
	Flaw remediation (ALC_FLR)
	Life cycle definition (ALC_LCD)
	Tools and techniques (ALC_TAT)
ATE: Tests	Coverage (ATE_COV)
	Depth (ATE_DPT)
	Functional tests (ATE_FUN)
	Independent testing (ATE_IND)
AVA: Vulnerability assessment	Covert channel analysis (AVA_CCA)
	Misuse (AVA_MSU)
	Strength of TOE security functions (AVA_SOF)
	Vulnerability analysis (AVA_VLA)

Table 1: Assurance family breakdown and mapping"

Evaluation assurance levels (chapter 11)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 11.1)

“Table 6 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in chapter 7 of this Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be extended with explicitly stated assurance requirements.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Configuration management	ACM_AUT				1	1	2	2
	ACM_CAP	1	2	3	4	4	5	5
	ACM_SCP			1	2	3	3	3
Delivery and operation	ADO_DEL		1	1	2	2	2	3
	ADO_IGS	1	1	1	1	1	1	1
Development	ADV_FSP	1	1	1	2	3	3	4
	ADV_HLD		1	2	2	3	4	5
	ADV_IMP				1	2	3	3
	ADV_INT					1	2	3
	ADV_LLD				1	1	2	2
	ADV_RCR	1	1	1	1	2	2	3
	ADV_SPM				1	3	3	3
Guidance documents	AGD_ADM	1	1	1	1	1	1	1
	AGD_USR	1	1	1	1	1	1	1
Life cycle support	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD				1	2	2	3
	ALC_TAT				1	2	3	3
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	2	2	3
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_CCA					1	2	2
	AVA_MSU			1	2	2	3	3
	AVA_SOF		1	1	1	1	1	1
	AVA_VLA		1	1	2	3	4	4

Table 6: Evaluation assurance level summary”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 11.3)

“Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation, and that it provides useful protection against identified threats.”

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 11.4)

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practice. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 11.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practices.

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed (chapter 11.6)

“Objectives

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practices which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 11.7)

“Objectives

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practices supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested (chapter 11.8)

“Objectives

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 11.9)

“Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.“

Strength of TOE security functions (AVA_SOF) (chapter 19.3)

“Objectives

Even if a TOE security function cannot be bypassed, deactivated, or corrupted, it may still be possible to defeat it because there is a vulnerability in the concept of its underlying security mechanisms. For those functions a qualification of their security behaviour can be made using the results of a quantitative or statistical analysis of the security behaviour of these mechanisms and the effort required to overcome them. The qualification is made in the form of a strength of TOE security function claim.”

Vulnerability analysis (AVA_VLA) (chapter 19.4)

"Objectives

Vulnerability analysis is an assessment to determine whether vulnerabilities identified, during the evaluation of the construction and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), could allow users to violate the TSP.

Vulnerability analysis deals with the threats that a user will be able to discover flaws that will allow unauthorised access to resources (e.g. data), allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

"Application notes

A vulnerability analysis is performed by the developer in order to ascertain the presence of security vulnerabilities, and should consider at least the contents of all the TOE deliverables including the ST for the targeted evaluation assurance level. The developer is required to document the disposition of identified vulnerabilities to allow the evaluator to make use of that information if it is found useful as a support for the evaluator's independent vulnerability analysis.”

“Independent vulnerability analysis goes beyond the vulnerabilities identified by the developer. The main intent of the evaluator analysis is to determine that the TOE is resistant to penetration attacks performed by an attacker possessing a low (for AVA_VLA.2 Independent vulnerability analysis), moderate (for AVA_VLA.3 Moderately resistant) or high (for AVA_VLA.4 Highly resistant) attack potential.”