

Secure Infrastructures for IT Systems

Infrastructure Measures for High Protection Requirements



Date:	28.02.05
Version:	2.5
Author:	Joachim Faulhaber
Evaluation criteria:	TSI V1.3

Table of Contents

1	INTRODUCTION	3
1.1	Business Success depends on IT	3
1.2	Hazard Potential	3
1.3	Physical Security	3
1.4	Targets	4
1.5	TSI	4
1.6	Application Area	4
1.7	Certification	5
1.8	Project Program.....	6
2	OVERVIEW OF THE EVALUATION ASPECTS	7
2.1	Documentation	7
2.2	Structural Circumstances	7
2.3	Security Systems.....	8
2.4	Power Supply	8
2.5	Fire Alarm and Fire-Fighting Systems	8
2.6	Ventilation Systems	8
2.7	Organization	8
3	EVALUATION CRITERIA	10
3.1	Documentation	11
3.2	Structural Circumstances	11
3.3	Security Systems.....	11
3.4	Power Supply	12
3.5	Fire Alarm and Fire-Fighting Systems	12
3.6	Ventilation Systems	12
3.7	Organization	12
4	INCREASED SECURITY PROTECTION REQUIREMENTS AS PER LEVEL3.....	13
5	CERTIFICATE AND TEST MARK	14
6	CERTIFICATION OF COMPUTER CENTERS	15
7	»TRUSTED SITE« CERTIFICATION FAMILY.....	16
8	GLOSSARY AND ABBREVIATIONS	17
9	CONTACTS.....	18

1 Introduction

1.1 Business Success depends on IT

Information and communication systems form the basis of a variety of entrepreneurial decisions and activities. Their availability is of fundamental significance for the company. Today, failures can quickly threaten the very existence of a company.

Time-critical accesses, just-in-time runs, a high degree of networking and on-line businesses require a high availability and increase the demands on the systems performance, the data management, and the corresponding infrastructure. This includes a tendency to centralize business-critical productive hardware. In order to reduce the probability of systems failures and data losses in such concentrated environments, sophisticated security concepts and reliable safety evaluations are required.

Also within the frame of the Basel II discussion, these evaluations are of special significance as in future targeted risk assessment is a prerequisite as regards the decision for lending and its conditions. In this context, banks and borrowers both benefit from a safety assessment of the IT infrastructures as the assessment allows reliable statements to enter into the risk assessment.

1.2 Hazard Potential

The hazard potential in the area of physical security is of a varied nature and its impacts serious. According to the IT-Grundschutzhandbuch des Bundesamts für Sicherheit in der Informationstechnik (BSI) (IT Baseline Protection Manual of the Federal Office for Information Security) the following four threat categories are assumed:

Force Major, e.g. lightning, fire, or water.

Organizational shortcomings, e.g. lack of or insufficient rules, or unauthorized access to rooms requiring protection.

Technical failures, e.g. disruption of power supply, failure of internal supply networks and of existing safety devices.

Deliberate acts, e.g. unauthorized entry into a building, theft, vandalism, and attacks.

1.3 Physical Security

The safety of IT systems can only be optimized as an integral security concept. The security aspects in the area of infrastructure, i.e. the physical security are just as important as the organizational security and the information technology security (IT systems and their applications). As regards the last mentioned security aspects, more and more procedures and solutions are

available (refer to chapter 6), the physical security, however, – besides the approaches in the IT Baseline Protection Manual – has rarely been assessed systematically.

This is the starting point for the **TÜV Informationstechnik GmbH** catalogue of criteria which helps to fully record, evaluate and assess the actual conditions directly.

1.4 Targets

The objective identification and adequate elimination of security risks in the IT infrastructure constitute an immediate matter of concern for any IT operator. The top priorities are to introduce preventive measures for the physical protection of IT and communication systems, and to ensure an infrastructure which meets the requirements on the basis of existing standards and capacity limits. The target is to ensure maximum system and data availability as well as a safety of almost 100 percent.

1.5 TSI

Based on its experience as certification service provider for the acceptance of Trust Centers for electronic signatures, TÜV-Informationstechnik GmbH (TÜViT) has developed a standard procedure for the evaluation of **secure infrastructures for IT Systems** which considers the acknowledged expert measures. The procedure forms part of the TÜViT certification program “Trusted Site“ and is called

Trusted Site Infrastructure (TSI)

The evaluation catalogue in the current version of V1.1 which is the basis of the procedure follows the catalogue of measures published by the Bundesamt für Sicherheit in der Informationstechnik (BSI) and the IT Baseline Protection Manual of the BSI and considers the applicable DIN standards, VDE regulations, and VdS publications.

The procedure allows the appropriate evaluation of the infrastructure which forms the basis of the IT installations, while placing special emphasis on the individual environment and on the complexity and dynamics of such installations.

1.6 Application Area

The application area of *Trusted Site Infrastructure*, however, is not restricted to IT and communication systems. Other values requiring protection in security storage rooms or archives also necessitate the implementation of infrastructure measures in order to protect them against access, or to meet requirements on the environment. The evaluation criteria to be considered (see chapter 2) generally also apply to these application areas.

The verification of the infrastructure by a neutral third party has a series of positive aspects:

- Security during the award process for the planning of a new computer centre, if certification is part of the tender.
- Trust certificate for the market positioning, as the award of a certificate documents the special efforts made in the field of the security measures and can be pointed out as a competitive advantage.
- Quality assurance and improvement while piloting the project and determining the position with regard to internal decision making processes.
- Positive influence on the rating of a company and therefore possibly a better starting point as regards capital procurement and insurance conditions.
- Assurance of trustworthiness of supervising institutions.

As a rule, all computer centers operators benefit from these advantages. Some aspects, however, especially concern ASPs, ISPs, Collocation providers, and industrial branches in their role as suppliers which are subject to extensive obligations as regards availability.

1.7 Certification

A certification can demonstrate the reliability of the system to a third party by simultaneously meeting the required protection targets, and it generates trust on the basis of a "Third Party Inspection".

The evaluation catalogue permits to evaluate the infrastructure and to derive availability statements for the IT installation hereof. By accepting the installed infrastructure components, the operator can be assured that he has taken all precautions considered as appropriate and necessary and that he has ensured that all components function together.

Three security levels can be certified (see Figure 1): Level1, Level2, and Level3.

For **Level1** a series of requirements is defined that must be met and explained by means of a description – in this case **D**ocumentation of the **I**nfrastructure **M**easures, called DIM.

On **Level2** a security concept replaces the DIM. This concept not only describes the measures taken but also how they work together, their benefit and their effective potential. Furthermore, the security concept describes the security targets and requirements, and provides a risk analysis. The evaluation procedure therefore bases on a detailed description and allows to carry out a comprehensive evaluation, thus creating an additional trust anchor.

Level3 considers further aspects, such as additional re-enforcements of the structural circumstances, improved fire protection installations, comprehensive

access control system, emergency power supply, and redundant design of further infrastructure components.

“**Level2 enhanced**” also indicates whether, in addition to the basic requirements of Level1 and the provision of a security concept, further requirements as per Level3 have been met.

Provided that appropriate IT and organizational measures have also been taken, yet the meeting of Level1 can crucially contribute to clearly minimize the probability of failure times over 24 hours.

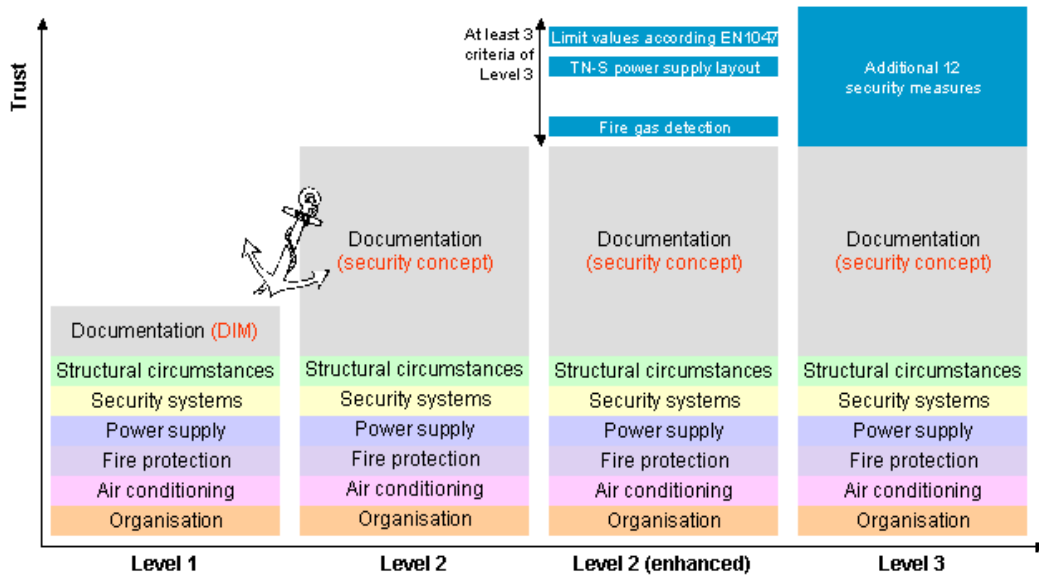


Figure 1: Assessment level of a TSI certification

1.8 Project Program

Generally, the project starts with a workshop or a kick-off meeting. On this occasion the evaluation aspects are described once again, the evaluation program is explained in detail, and the structure and significance of a security concept are described. Furthermore, a first site visit takes place to determine the possibility of testing or to point out obvious differences.

After the workshop the interested party can decide whether it wants an evaluation to be carried out or not. If yes, a DIM or **Security Concept Document (SCD)** has to be submitted for detailed testing. On the basis of the documentation the extent, the effect and the consistent application of the measures will be examined and commented on. The customer will have the opportunity to revise the document and eliminate detected weaknesses.

After the revision, the documentation will form the basis of the evaluation process. Then a site audit (application testing) will be agreed upon in the course of which it will be examined whether the measures and components have been implemented and/or applied as described.

Then, TÜViT prepares a test report for the customer and, provided that all requirements have been met, issues a certificate that authorizes to use the corresponding test mark.

2 Overview of the Evaluation Aspects

The obtained security level of an IT infrastructure is determined on the basis of minimum requirements which have been complied with. The following **Evaluation aspects** form part of the examination (see Figure 2).

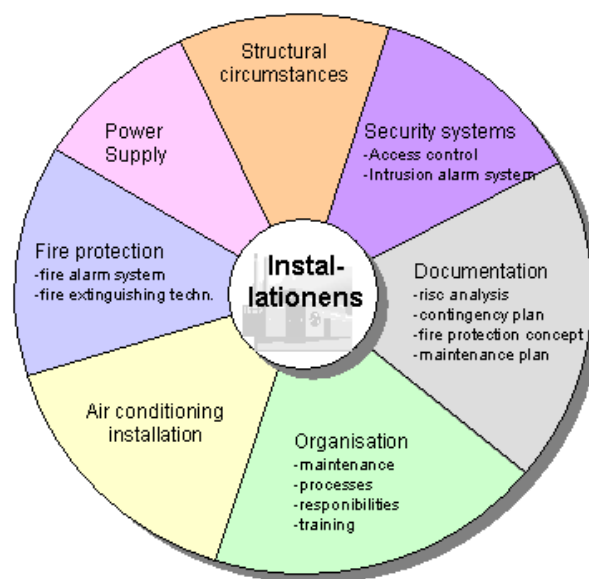


Figure 2: Evaluation aspects of the TSI certification

2.1 Documentation

The examination of the measures and of the infrastructure installed under the aspect of the sustainability can only be carried out within the context of a documented risk analysis or security concept. It forms the basis for the derivation of type and extent of proactive measures and is used to evaluate and to clearly show the hazard potential in case of a failure of the IT systems for a company.

After all, the infrastructure installation will only comply with the related requirement of availability, if rules of conduct exist and up-to-date plans and documentation are available in the case of emergency, thus enabling a rapid, expert and safe response.

For this reason, the documentation should not be restricted to a description of infrastructure measures (DIM), but be enhanced to form a comprehensive security concept (SCD).

2.2 Structural Circumstances

The building surrounds the IT and thus guarantees external protection. When considering the surrounding hazard potentials, the location of the building and the location of the security area within the building are both important in order to avoid a priori any existing potential sources of danger. Structural security aspects concern a. o. things the design of walls, doors, windows, external protection against lightning and fire lobbies as well as the routing of supply lines.

2.3 Security Systems

The security systems shall provide protection against deliberate acts. This includes, for instance, an access control system which not only controls the access to the security area but also infrastructure components, as e.g. distributor cabinets. An intrusion alarm system is necessary to early detect theft (hardware and data), sabotage, and vandalism, to deter subjects and to start countermeasures in time.

2.4 Power Supply

The power supply is essential for IT systems. It feeds the most different consumers and is subject to permanent change. The electrical installations are to be realized in accordance with the relevant DIN standards and VDE regulations, to be protected against over voltage, provided with adapted separations and protection of the electric circuits, and in addition precautions have to be taken for extensions. The dependencies of the IT systems from the infrastructure components require an uninterruptible power supply and an extensive emergency power supply which also includes telecommunication, security and air conditioning systems.

2.5 Fire Alarm and Fire-Fighting Systems

The risk factors fire and flue gas can be monitored by means of fire alarm systems, highly sensitive fire early warning systems and gas extinguishing systems. Under this aspect, it is important that the fire detection sensor system takes into account all security areas and that it is correctly located. Apart from signaling an alarm, shutdown functions and damage containment measures such as a gas extinguishing system must be triggered to quickly contain a fire. A fire protection concept shall be coordinated with the local fire brigade.

2.6 Ventilation Systems

IT systems as well as archives depend on specified ambient conditions. It has to be ensured that air temperature, humidity and dust content comply with specified limit values. To ensure its availability, air conditioning is necessary in redundant design.

2.7 Organization

IT infrastructure components can break down, too. The regular check of their condition, properties and behavior is necessary to prove the permanent effectiveness and availability of the infrastructure components in accordance with the security requirements. The responsibilities must be clearly defined. Likewise, rules must be established which provide for access rights to be defined, side effect evaluations to be initiated and the training of personnel to be ensured when the infrastructure components are being enhanced. The regular backup of data on optical or magnetic media also is considered to be of essential importance.

3 Evaluation Criteria

For each of the evaluation aspects listed in chapter 2, a series of defined criteria exists which determines the requirements for a “*Trusted Site Infrastructure*“. A short listing of these requirements together with all partial aspects considered in the evaluation procedure are presented in Table 1 and further explained in the following sections.

Table 1: Partial aspects - details of the evaluation aspects

Evaluation aspect	Partial aspect
Documentation	<ul style="list-style-type: none"> • DIM or security concept • Fire protection concept • Contingency plan / restart plan • Maintenance plan • Rules (access, extensions)
Structural Circumstances	<ul style="list-style-type: none"> • Environment (location and plans) • Construction (walls, doors, and windows) • External lightning protection • Structural fire protection • Protection of the supply lines
Security Systems	<ul style="list-style-type: none"> • Access control system (type, field of application, identification, relaying) • Intrusion detection system (type, field of application, relaying)
Power Supply	<ul style="list-style-type: none"> • Diagrams • Supply • Main distribution centre • Rating / design • UPS • Over voltage protection
Fire Alarm and Fire-Extinguishing Systems	<ul style="list-style-type: none"> • Type and operation of the fire alarm technology • Gas extinguishing system • Fire protection
Ventilation Systems	<ul style="list-style-type: none"> • Air conditioning • Monitoring of limit values • Fire and smoke flaps

Evaluation aspect	Partial aspect
-------------------	----------------

- | | |
|---------------------|--|
| Organization | <ul style="list-style-type: none">• Functional tests• Maintenance• Processes• Distribution of rooms• Responsibilities• Training |
|---------------------|--|

3.1 Documentation

In the security concept weaknesses and hazard potentials are identified, risk factors derived hereof, and measures defined. Subsequently, the risk factors are assessed. The security concept provides an overview of the values requiring protection and describes all application measures for the aspects listed in Table 1. Rules must be written down and known to the staff concerned within the company. If necessary, maintenance plans must be covered by appropriate contracts. In case of Level1 a security concept is not required, the security measures, however, are described in a summarized way in a documentation (DIM).

3.2 Structural Circumstances

Walls, doors and windows must offer protection against access, fire and debris (DIN V ENV 1627). It has also to be ensured that building sections threatened by water, EM/RF interference fields (EN 50147 part 1), and dangerous next-door production processes are avoided. The building must be protected against lightning and allow for the security area to be located in a separate fire protection area (DIN 4102). The supply lines have to be laid in protective constructions. Level3 specifies that in order to ensure the functioning of the IT systems and of the data media in case of fire, the objects requiring protection may only be exposed to defined maximum temperature and humidity limits (following EN-1047-1 and EN-1047-2).

3.3 Security Systems

An access control system including appropriate access rules must exist not only for the security area but also for all infrastructure components (e.g. distributor) (VdS 2358). The protection against breaking and entering must feature several levels, and all security sensitive areas must be monitored by means of an intrusion detection system (VdS 2311). This includes connecting these installations to the emergency power supply and to a permanently manned control room.

3.4 Power Supply

As regards the supply it has to be ensured that alternative possibilities exist, such as a ring feeder connection. The electrical installation in the complete building should be a TN-S-system layout, otherwise special precautions for the electrical distribution have to be taken. As a rule, the supply of the IT devices must be separate from the supply of other consumers. It is necessary that the over voltage protection features at least two levels and that there is a UPS. For Level3, an installation for emergency power supply (NEA) or a similar protection must be provided.

3.5 Fire Alarm and Fire-Fighting Systems

A fire alarm system (VdS 2095) in two line design has to be installed in the complete security area and linked with the fire brigade. Side rooms, double floors, suspended ceilings and air ducts must also be included in the fire monitoring. Apart from signaling an alarm it is also important that damage containment measures such as a gas extinguishing system in the security area or other appropriate measures are triggered.

3.6 Ventilation Systems

Likewise to the redundant design of the installation and the monitoring of the limit values it also must be ensured that the installation is integrated into the fire protection concept, which includes the external capacitors for the lightning protection. The installation must be located in a protected area.

3.7 Organization

Procedural instructions govern the testing of the electrical installation design in case of an extension. Periodical functional tests must be carried out for all safeguards. An equipment schedule defines maintenance methods and intervals for the wear parts of the infrastructure components and IT hardware. Even in case of a telecommunication system failure, the communication with the exterior is ensured. The data backup media must be stored and protected against fire and access in an area separate from the security area, and the media must be sufficiently protected as per EN1047.

4 Increased Security Protection Requirements as per Level3

If even shorter downtimes are required (refer to chapter 1) the measures for the high protection requirements as per Level3 will lead to the appropriate effect. This includes additional provisions on the structural and technical side. Table 2 shows the extended partial aspects:

Table 2: Further partial aspects for high protection requirements Level3

Evaluation Aspects	Partial Aspects
Documentation	<ul style="list-style-type: none"> • <i>No further measures</i>
Structural Circumstances	<ul style="list-style-type: none"> • Risk analysis environment • Increased resistance of windows and doors against intrusion • Temperature and humidity limit values for systems and data media (EN 1047)
Security Systems	<ul style="list-style-type: none"> • Access control system (identification, logging, monitoring of the locking condition, video system) • Intrusion detection system (motion detector) • Protection of the supply lines
Power Supply	<ul style="list-style-type: none"> • TN-S system • Redundant design of central UPS • Installation for emergency power supply (NEA) • Emergency power supply for all infrastructure components • Functional integrity of the cables (E90) from main distribution to sub-distribution
Fire Alarm and Fire Extinguishing Systems	<ul style="list-style-type: none"> • Air sampling smoke detection system
Ventilation Systems	<ul style="list-style-type: none"> • Smoke detector and escape flap at the fresh air aspiration duct
Organization	<ul style="list-style-type: none"> • Adapted maintenance contracts • Requirements and tests in case of system extensions
Other	<ul style="list-style-type: none"> • Smoke tightness (DIN 18095 Part 2) • Redundant design of the data networks

5 Certificate and Test Mark

On the basis of the evaluation criteria for *Trusted Site Infrastructure* (see chapter 3) and provided that all partial aspects of the examined security area have been met, it will be possible to issue a certificate (Figure 3) that entitles to use the test mark "*Trusted Site Infrastructure*" (see cover sheet). The evaluation aspects listed in chapt. 2 are imprinted on the backside of the certificate. The certificate is valid for two years and can be extended. The operator may use the test mark on his WEB site as well as for brochures. Furthermore, provided that the customer gave his consent, the test mark and the certificate will be published at www.tuvit.de and www.certuvit.de, respectively.



Figure 3: certificate sample

6 Certification of Computer Centers

As already indicated above, a computer centre can only be considered as safe if appropriate physical, organizational and IT security measures have been taken. Apart from the test program for physical security, TÜVIT also covers the other aspects with further test programs, so that this modular TÜVIT scheme allows to represent a comprehensive statement on the safety and quality of the operation of a computer centre.

Trusted Site Security analyses the network security and the quality of the system hardening in order to cover the IT security aspects. *Trusted Site ITIL* extends the view to the processes of IT Service Management and examines as per BS15000 its quality, integrity and level of implementation.

The test programs complement each other due to their different focus. Their combination leads to an integral examination and furnishes universal proof of security and quality for the operator in the form of three certificates which document that all aspects have been considered and security measures have been implemented on a consistently high level for all three cornerstones in the security domain as well as in the quality domain (see Figure 4).

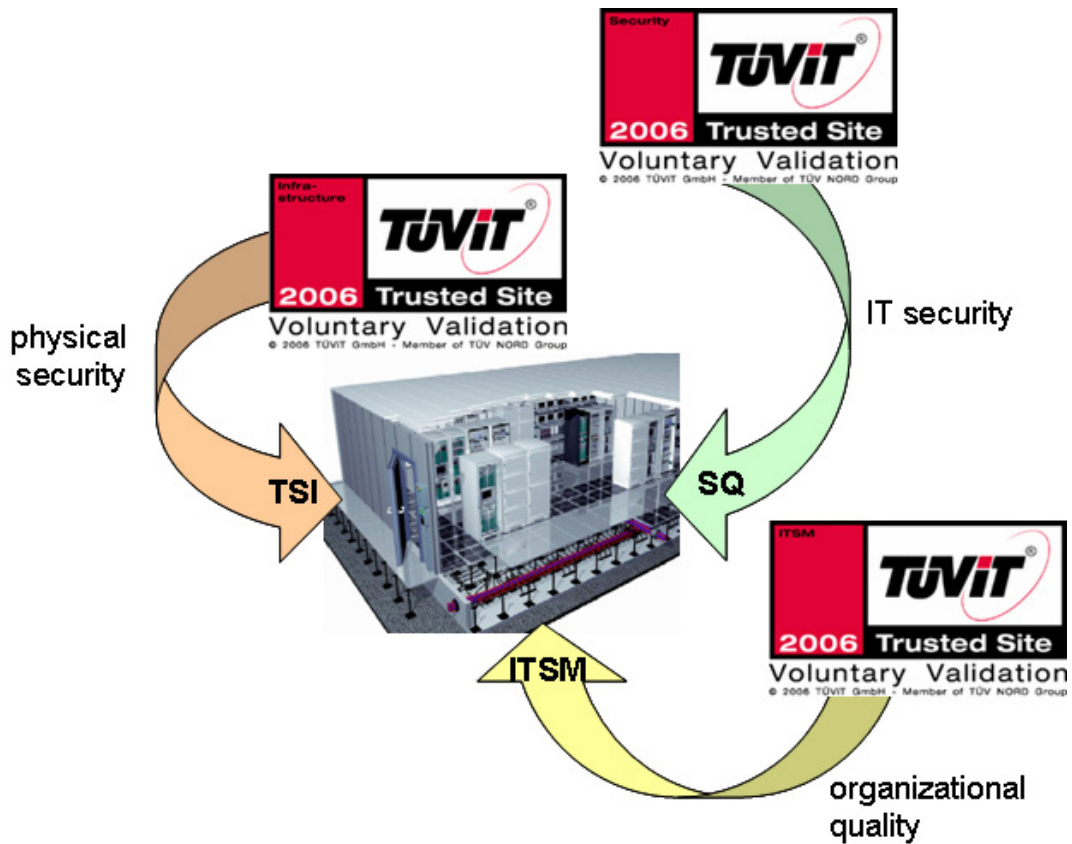


Figure 4: Certification of computer centers

7 »Trusted Site« Certification Family

Under the logo »*Trusted Site*«, TÜV Informationstechnik GmbH issues test marks that confirm the compliance with security and quality characteristics for IT systems.



Trusted Site — *Infrastructure*

examines the infrastructure (building, power supply, security systems, fire alarm and fire extinguishing systems, etc.) and confirms the suitability of security areas which require a high availability.



Trusted Site — *Security*

examines the IT security of (typically inter-connected) IT installations and confirms the compliance with appropriate security targets within the frame of a security qualification.



Trusted Site — *ITSM*

examines the IT Service Management Processes of the ITIL Reference model concerning quality, integrity and level of implementation in reference to the requirements of BS 15000 for the organization.



Trusted Site — *Privacy*

examines the privacy of a process and combines it with a security analysis which evaluates the security of the relevant IT installation.

In the case of a matching duration and a matching area of inspection, the above mentioned TÜVIT test marks can also be awarded as a combination of test marks.

8 Glossary and Abbreviations

ASP	Application Service Provider
BLA	Fire extinguishing system
BMA	Fire alarm system
BSI	Federal Agency for IT Security
DIM	Documentation of the infrastructure measures
Infrastructure components	Any technical building enlargement, e.g. NEA, EMA, BLA, BMA, USV, ZKA, etc., are infrastructure components
ISMS	Information security management system
ISP	Internet Service Provider
ITIL	IT Infrastructure Library
EMA	Intrusion detection system
NEA	Emergency installation for emergency power supply
RegTP	Regulation Authority for telecommunications and mail
Security area	The object of inspection whose security is to be assured by using procedures and measures for a supporting and secure infrastructure.
SigG	Signature Act
Siko	Security concept
TK system	Telecommunications system / private branch exchange
TN-S system	Special design of the electrical installation as regards the grounding. As regards the TN-S system, a protective conductor which is separate from the neutral conductor or from the grounded phase.
TSI	Trusted Site Infrastructure
UPS	Uninterruptible Power Supply
ZKA	Access control installation

9 Contacts

Dipl.-Inform. Joachim Faulhaber

Certification

TÜV Informationstechnik GmbH
Member of TÜV NORD Group
Langemarckstrasse 21
45141 Essen, Germany

Tel.: +49 201 8999-584
Fax: +49 201 8999-555
J.Faulhaber@tuvit.de
<http://www.tuvit.de>

Germany

Dr. Ernst-Hermann Gruschwitz

Head of Certification

TÜV Informationstechnik GmbH
Member of TÜV NORD Group
Langemarckstrasse 21
45141 Essen, Germany

Tel.: +49 201 8999-580
Fax: +49 201 8999-555
E.Gruschwitz@tuvit.de
<http://www.tuvit.de>

Germany