

Christopher Eller
Bennet Vogel

Information Security and Prototype Protection According to ISA 6 & TISAX®

Understand and Implement Requirements Successfully



HANSER

Eller / Vogel

**Information Security and Prototype Protection
According to ISA 6 & TISAX®**

Christopher Eller
Bennet Vogel

Information Security and Prototype Protection According to ISA 6 & TISAX®

Understand and Implement Requirements Successfully

HANSER

TISAX® is a registered trademark of the ENX Association.

VDA® is a registered trademark of the German Association of the Automotive Industry.



Print-ISBN: 978-1-56990-496-1

E-Pub-ISBN: 978-1-56990-962-1

E-Book-ISBN: 978-1-56990-959-1

All information, procedures, and illustrations contained in this work have been compiled to the best of our knowledge and is believed to be true and accurate at the time of going to press. Nevertheless, errors and omissions are possible. Neither the authors, editors, nor publisher assume any responsibility for possible consequences of such errors or omissions. The information contained in this work is not associated with any obligation or guarantee of any kind. The authors, editors, and publisher accept no responsibility and do not assume any liability, consequential or otherwise, arising in any way from the use of this information – or any part thereof. Neither do the authors, editors, and publisher guarantee that the described processes, etc., are free of third party intellectual property rights. The reproduction of common names, trade names, product names, etc., in this work, even without special identification, does not justify the assumption that such names are to be considered free in the sense of trademark and brand protection legislation and may therefore be used by anyone.

The final determination of the suitability of any information for the use contemplated for a given application remains the sole responsibility of the user.

Bibliographic information of the German National Library:

The German National Library lists this publication in the German National Bibliography; detailed bibliographic data are available on the Internet at <http://dnb.d-nb.de>.

This work is protected by copyright.

All rights, including those of translation, reprint, and reproduction of the work, or parts thereof, are reserved. No part of this work may be reproduced in any form (photocopy, microfilm, or any other process) or processed, duplicated, transmitted, or distributed using electronic systems, even for the purpose of teaching – with the exception of the special cases mentioned in §§ 53, 54 UrhG (German Copyright Law) – without the written consent of the publisher.

No part of the work may be used for the purposes of text and data mining without the written consent of the publisher, in accordance with § 44b UrhG (German Copyright Law).

© 2026 Carl Hanser Verlag GmbH & Co. KG, Munich

Vilshofener Straße 10 | 81679 Munich | info@hanser.de

www.hanserpublications.com

www.hanser-fachbuch.de

Editor: Lisa Hoffmann-Bäumel

Production Management: Eberl & Koesel Studio, Kempten

Cover concept: Marc Müller-Bremer, www.rebranding.de, Munich

Cover design: Max Kostopoulos

Cover picture: [shutterstock.com/Gorodenkoff](https://www.shutterstock.com/Gorodenkoff)

Typesetting: le-tex publishing services GmbH, Leipzig

Printed and bound by: CPI Books GmbH, Leck

Content

Foreword to the English edition	XI
Foreword to the 2nd edition	XIII
Preface to the 1st edition	XV
1 IS Policies and Organization.....	1
1.1 Information security policies	1
1.1.1 To what extent are information security policies available?	1
1.2 Organization of information security	4
1.2.1 To what extent is information security managed within the organization?	4
1.2.2 To what extent are information security responsibilities organized?	7
1.2.3 To what extent are information security requirements considered in projects?	10
1.2.4 To what extent are the responsibilities between external IT service providers and the own organization defined?	12
1.3 Asset management	15
1.3.1 To what extent are information assets identified and recorded? ..	15
1.3.2 To what extent are information assets classified and managed in terms of their protection needs?	17
1.3.3 To what extent is it ensured that only evaluated and approved external IT services are used for processing the organization's information assets?	20
1.3.4 To what extent is it ensured that only evaluated and approved soft- ware is used for processing the organization's information assets?	22

1.4	Risk management for information security	24
1.4.1	To what extent are information security risks managed?	24
1.5	Assessment	28
1.5.1	To what extent is compliance with information security ensured in procedures and processes?	28
1.5.2	To what extent is the ISMS reviewed by an independent authority?	30
1.6	Incident and crisis management	32
1.6.1	To what extent are information security relevant events or observations reported?	32
1.6.2	To what extent are reported security events managed?	35
1.6.3	To what extent is the organization prepared to handle crisis situations?	38
2	Human Resources	43
2.1	Personnel management	43
2.1.1	To what extent is the qualification of employees for sensitive work fields ensured?	43
2.1.2	To what extent is all staff contractually bound to comply with information security policies?	47
2.1.3	To what extent is staff made aware of and trained with respect to the risks arising from the handling of information?	48
2.1.4	To what extent is mobile work regulated?	50
3	Physical Security	53
3.1	Physical security and business continuity	53
3.1.1	To what extent are security zones managed to protect information assets?	53
3.1.2	(Replaced)	57
3.1.3	To what extent is the handling of supporting assets managed? ...	57
3.1.4	To what extent is the handling of mobile IT devices and mobile data storage devices managed?	58
4	Identity and Access Management	61
4.1	Identity management	61
4.1.1	To what extent is the use of identification means managed?	61
4.1.2	To what extent is the user access to IT services and IT systems secured?	63

4.1.3	To what extent are user accounts and login information securely managed and applied?	65
4.2	Access management	69
4.2.1	To what extent are access rights assigned and managed?	69
5	IT Security/Cyber Security	71
5.1	Cryptography	71
5.1.1	To what extent is the use of cryptographic procedures managed?	71
5.1.2	To what extent is information protected during transfer?	74
5.2	Operations security	76
5.2.1	To what extent are changes managed?	76
5.2.2	To what extent are development and testing environments separated from operational environments?	78
5.2.3	To what extent are IT systems protected against malware?	79
5.2.4	To what extent are event logs recorded and analysed?	82
5.2.5	To what extent are vulnerabilities identified and addressed?	85
5.2.6	To what extent are IT systems and services technically checked (system and service audit)?	86
5.2.7	To what extent is the network of the organization managed?	89
5.2.8	To what extent is continuity planning for IT services in place? ...	91
5.2.9	To what extent is the backup and recovery of data and IT services guaranteed?	95
5.3	System acquisition, requirements management and development	97
5.3.1	To what extent is information security considered in new or further developed IT systems?	97
5.3.2	To what extent are requirements for network services defined? ..	100
5.3.3	To what extent is the return and secure removal of information assets from external IT services regulated?	102
5.3.4	To what extent is information protected in shared external IT services?	103
6	Supplier Relationships	105
6.1	Supplier relationships	105
6.1.1	To what extent is information security ensured for contractors and cooperation partners?	105
6.1.2	To what extent is non-disclosure regarding the exchange of information contractually agreed?	108

- 7 Compliance 111**
 - 7.1 Aligning the company with laws and guidelines 111
 - 7.1.1 To what extent is compliance with regulatory and contractual provisions ensured? 111
 - 7.1.2 To what extent is the protection of personally identifiable data considered when implementing information security? 116
- 8 Prototype Protection 119**
 - 8.1 Physical and environmental security 119
 - 8.1.1 To what extent is a security concept available describing minimum requirements regarding the physical and environmental security for prototype protection? 120
 - 8.1.2 To what extent is perimeter security existent preventing unauthorized access to protected property objects? 122
 - 8.1.3 To what extent is the outer skin of the protected buildings constructing such as to prevent removal or opening of outer-skin components using standard tools? 123
 - 8.1.4 To what extent is view and sight protection ensured in defined security areas? 124
 - 8.1.5 To what extent is the protection against unauthorized entry regulated in the form of access control? 125
 - 8.1.6 To what extent are the premises to be secured monitored for intrusion? 126
 - 8.1.7 To what extent is a documented visitor management in place? ... 127
 - 8.1.8 To what extent is on-site client segregation existent? 128
 - 8.2 Organizational requirements 130
 - 8.2.1 To what extent are non-disclosure agreements/obligations existent according to the valid contractual law? 130
 - 8.2.2 To what extent are requirements for commissioning subcontractors known and fulfilled? 131
 - 8.2.3 To what extent do employees and project members evidently participate in training and awareness measures regarding the handling of prototypes? 132
 - 8.2.4 To what extent are security classifications of the project and the resulting security measures known? 133
 - 8.2.5 To what extent is a process defined for granting access to security areas? 133

8.2.6 To what extent are regulations for image recording and handling of created image material existent? 134

8.2.7 To what extent is a process for carrying along and using mobile video and photography devices in(to) defined security areas established? 135

8.3 Handling vehicles, components and parts 136

8.3.1 To what extent are transports of vehicles, components or parts classified as requiring protection arranged according to the customer requirements? 136

8.3.2 To what extent is it ensured that vehicles, components, and parts classified as requiring protection are parked/stored in accordance with customer requirements? 139

8.4 Requirements for test vehicles 139

8.4.1 To what extent are the predefined camouflage regulations implemented by the project members? 140

8.4.2 To what extent are measures for protecting approved test and trial grounds observed/implemented? 140

8.4.3 To what extent are protective measures for approved test and trial drives in public observed/implemented? 141

8.5 Requirements for events and shootings 141

8.5.1 To what extent are security requirements for presentations and events involving vehicles, components or parts classified as requiring protection known? 142

8.5.2 To what extent are the protective measures for film and photo shootings involving vehicles, components or parts classified as requiring protection known? 142

The Authors 143

Index 145

Foreword to the English edition

With currently over 50,000 certified locations, TISAX[®] has become the second largest standard for Information Security worldwide.

TISAX[®] is a label used to demonstrate the fulfilment of safety requirements set by large automotive companies and does not only apply to “typical suppliers” in the automotive sector. Virtually every company that supplies a European OEM (Original Equipment Manufacturer) or major supplier is already obliged to fulfil OEM requirements. This affects companies of all kinds: in addition to suppliers of automotive parts, also advertising agencies, management consultancies, photographers, software companies and many more.

The requirements of automotive manufacturers are published in a standard-like format as the “ISA catalogue” (ISA: Information Security Assessment), relate to information security and are therefore – apart from the special case of prototype protection – useful for almost every company. Companies with the TISAX[®] label generally achieve a level of information security comparable to ISO 27001 and in many cases even higher.

With the English edition of this book, we are responding to the growing demand from companies worldwide for a practical guide to implementing TISAX. Based on our second German edition, this book provides up to date information based on the latest version of the ISA Catalogue: We cover all Information Security and Prototype Protection requirements of this catalogue.

This book is based on the currently valid version 6.0.3 of the ISA catalogue, including the criteria catalogues “Information Security & Prototype Protection” (as of June 2025).

We have written the book in clear, practice-oriented language that is understandable without prior knowledge. Our aim is to enable the best possible understanding of the TISAX[®] requirements while providing directly implementable recommendations.

Darmstadt and Berlin, summer 2025

Christopher Eller

Bennet Vogel

Notes

This work addresses the “Information Security Assessment” standard in version 6.0.3:

- Publisher: © 2023 ENX Association, an Association under the French Law of 1901, registered under No. w923004198 at the Sous-préfecture of Boulogne-Billancourt, France.
- The “Data Protection” tab is provided, owned and copyrighted by VERBAND DER AUTOMOBILINDUSTRIE e. V. (VDA, German Association of the Automotive Industry); Behrenstr. 35; 10117 Berlin
- Source: <https://portal.enx.com/de-de/TISAX/downloads>
- This work is licensed under the Creative Commons Attribution-NoDerivatives 4.0 International Public License.

In the text of the book, chapter headings and the boxes labeled “Quotation from the VDA® ISA 6.0.3” cite this standard. The organizational structure of the book is based on the standard.

The authors of this book are not part of or affiliated with VDA® or ENX®. The following trademarks are mentioned:

- TISAX® is a registered trademark of the ENX® Association.
- VDA® is a registered trademark of the German Association of the Automotive Industry.
- ISO is a registered trademark of the International Organization for Standardization.
- DIN is a registered trademark of the German Institute for Standardization.



The VDA has updated the “Information Security Assessment” and made it available for download. Available at <https://portal.enx.com/de-de/TISAX/downloads>.

Foreword to the 2nd edition

The ISA catalogue in version 6 has been mandatory for new TISAX assessments since spring 2024.

The new version of the standard was first published primarily and initially in English and is now available directly on the ENX[®] website. The addition of “VDA[®]” of “VDA ISA” has already been largely dropped in the publications, and ENX[®] itself now only refers to the catalogue as “ISA” in many places. This is a clear sign that TISAX[®] will be used even more widely in the European automotive industry in the future.

It is now also possible to present the certification achieved, for example on the website or on a certificate in the entrance area, thanks to a “decorative document”: <https://portal.enx.com/en-us/news/New-decorative-TISAX-assessment-document-now-available>

With the 2nd edition of this book, we are updating our recommendations for implementing the standard and expanding them to include the prototype protection module. We provide implementation recommendations for all new information security requirements from ISA 6. Organizations that handle physical prototypes in accordance with TISAX[®] requirements will now also find implementation recommendations for this that are compatible with the recommendations for information security.

Feedback on the 1st edition as well as typical questions that were brought to us in discussions with consulting clients and audits have also been incorporated into the 2nd edition. We are grateful for this valuable input, which has enabled us to make the book even more practice-orientated.

Interest in TISAX[®] continues to be high in Germany, even from companies that have had no previous contact with the topic, and we are also receiving an increasing number of international enquiries. With the 2nd edition of the book, we want to give even more companies easy access to TISAX[®].

We have based this book on the currently valid version 6.0.2 of the ISA catalogue with the criteria catalogues “Information Security & Prototype Protection” (as of August 2024).

Darmstadt and Berlin, summer 2024

Christopher Eller

Bennet Vogel

Notes

This work deals with the “Information Security Assessment” standard in version 6.0.2:

- Publisher: © 2023 ENX Association, an Association according to the French Law of 1901, registered under No. w923004198 at the Sous-préfecture of Boulogne-Billancourt, France.
- The “Data Protection” tab is provided, owned and copyrighted by VERBAND DER AUTOMOBILINDUSTRIE e. V. (VDA, German Association of the Automotive Industry); Behrenstr. 35; 10117 Berlin
- Source: <https://portal.enx.com/de-de/TISAX/downloads>
- This work is licensed under the Creative Commons Attribution-NoDerivatives 4.0 International Public Licence.

In the text of the book, the chapter headings and the boxes “Quotation from the VDA® ISA 6.0.2” quote from this standard. The organizational structure of the book is based on the standard.

The authors of this book are not part of or affiliated with VDA® or ENX®. The following trademarks are mentioned:

- TISAX® is a registered trademark of the ENX® Association.
- VDA® is a registered trademark of the German Association of the Automotive Industry.
- ISO is a registered trademark of the International Organization for Standardization.
- DIN is a registered trademark of the German Institute for Standardization.



The VDA has updated the “Information Security Assessment” and made it available for download. Available at <https://portal.enx.com/de-de/TISAX/downloads>.

Preface to the 1st edition

TISAX® is a label used to demonstrate the fulfilment of security requirements of large German automotive companies and does not apply only to “typical suppliers” in the automotive sector.

The requirements of automotive manufacturers are published in a standard-like manner as the “VDA® ISA Catalogue” (VDA: German Association of the Automotive Industry; ISA: Information Security Assessment), relate to information security and are therefore – apart from the special case of prototype protection – useful for almost every company. Companies with the TISAX® label generally achieve a level of information security comparable to ISO 27001 and in many cases even higher.

Virtually every company that supplies an OEM (Original Equipment Manufacturer) or major supplier is already obliged to fulfil the requirements of OEMs or will be in the near future. This affects companies of all kinds: In addition to suppliers of automotive parts, this also includes advertising agencies, management consultancies, photographers, software houses and many more.

The content of the VDA® ISA catalogue is based on the ISO 27001 standard. Older editions of the VDA® ISA up to version number 4 therefore have a similar chapter structure. Version 5 of the VDA® ISA catalogue introduced a completely new chapter structure. The link to ISO 27001 is no longer recognizable at first glance. This “cutting of the cord” from ISO 27001 speaks for the increased self-confidence of ENX® and VDA® in having established a success story with TISAX®.

If you are already familiar with ISO standards and the usual audit procedures, much of the “TISAX® world” will also seem familiar to you. There is also a standard here, but in the form of an Excel spreadsheet in which you can directly enter information on the implementation of the standard requirements. There are also audits – referred to here as inspections – but only once every three years. Instead of a DAkkS, the ENX® has overall supervision of the authorized certification bodies – which are known as