



# TISAX - Trusted Information Security Assessment Exchange

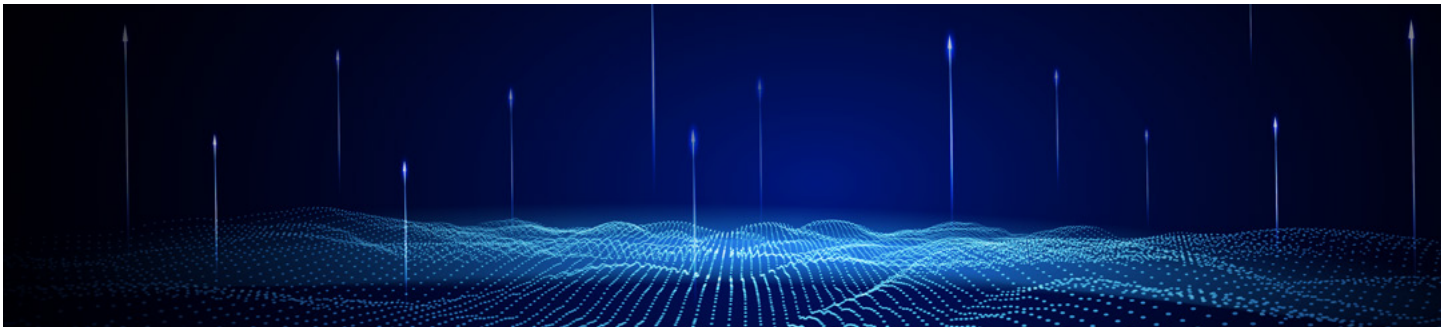
KPMG Cybersecurity

KPMG China

---

[kpmg.com/cn](https://kpmg.com/cn)





## Securing protectable information within the automotive supply chain

TISAX(Trusted Information Security Assessment Exchange) is originated from the internal information security audits of German automotive OEMs for its suppliers in order to evaluate an adequate level of information security within the entire automotive supply chain. It has been gradually expanded to German automotive industry through VDA (providing the information security standards) & ENX (providing the platform for the TISAX registration, Label exchange and accreditation for the TISAX audit providers) and has established a common assessment and exchange mechanism for evaluating supplier's information security capabilities. TISAX and the corresponding information security assessment were introduced in 2017 and became mandatory for automotive suppliers. Automotive suppliers (providing parts, components, services etc.) must implement and maintain an

Information Security Management System (ISMS), afterwards pass the corresponding level of TISAX audit in order to further be contracted by an OEM and/or enter the German automotive market.

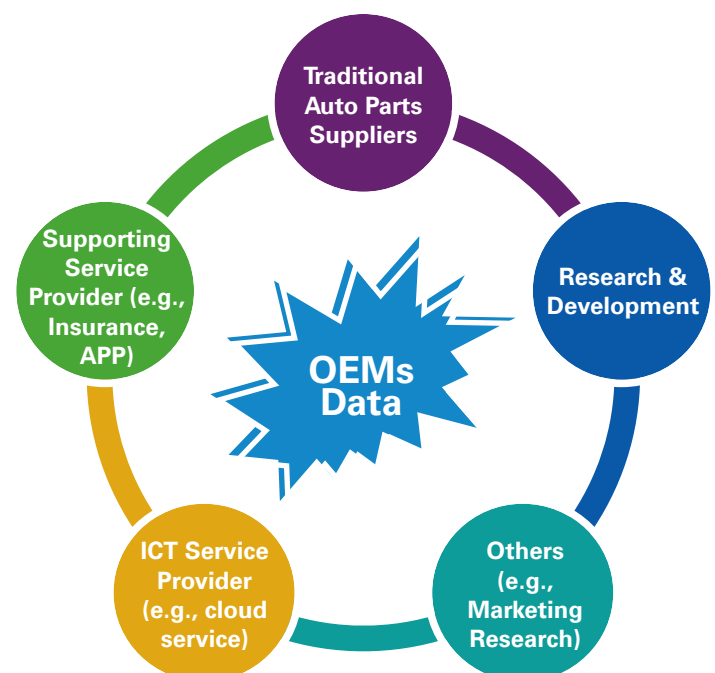
KPMG AG Wirtschaftsprüfungsgesellschaft, as an ENX accredited TISAX audit service provider, enjoys good reputation globally with professional audit experience. KPMG China strictly follows our global cyber service standard and internal TISAX audit process who can provide one-stop service to Chinese clients. Due to the mutual teamwork of the German and Chinese KPMG TISAX professionals, the service carried out by KPMG minimizes communication costs, audit cycles and increases efficiency in the entire audit process incl. achieving the TISAX label. We are also able to provide customized services according to the needs of clients.

## Traditional Suppliers ➔ Broader Business Partners

The participants within the TISAX process are in general classical parts and/or components manufacturer on domestic and multinational companies. The locations which are subject to a TISAX audit include R&D centers, Headquarters, office locations, laboratories as well as production factories and test areas.

As the car itself evolves to become more climate efficient and digital, companies in the field of new energy vehicles, mobile internet and autonomous driving with its corresponding technical R&D as well as related services became also an indispensable part of the automotive supply chain. Many more well know tech giants as well as highly innovative start-ups started their TISAX journey.

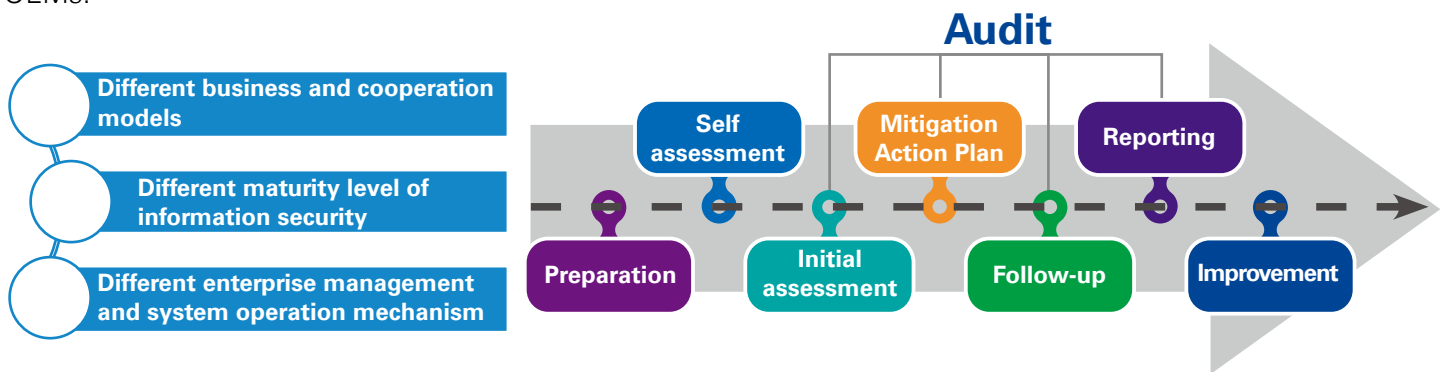
Furthermore, companies engaging in market research and/or customer centric services (like research agencies) as well as companies providing supporting ICT services (including system operation, mail services, cloud services etc.) also needs to provide a valid TISAX label to its OEM-clients and/or automotive clients.





## TISAX Journey: Registration → Audit → Mitigation → Confirmation → Report → Share

According to the requirements, participants initially need to register the from OEM-side pre-defined scope (incl. locations and assessment objects) on the ENX platform. KPMG as a third party audit provider will conduct the assessment based on the pre-defined scope, and issue a TISAX audit report with signature which will be uploaded onto ENX platform. Participants then will obtain the TISAX Label (valid for 3 years) as a necessary condition for suppliers to apply for purchase order, project cooperation, system account, and supplier qualification renewal from OEMs.



## TISAX assessment objective, level and maturity scoring

In addition to Information Security based on ISO/IEC 27001 and 27002, TISAX audit may include three other assessment objectives: prototype protection, connection to third parties and data protection. According to the sensitivity of the information obtained, processed and stored by suppliers, the protection need could be high (AL2) or very high (AL3). Note that AL3, AL 2 with prototype protection or AL2 with connection to third parties mandatorily requires an on-site audit. These audits include classical audit procedures like interviews, on-site inspection, evidence confirmation, etc..

The audit result is expressed in a maturity level thereby strictly following the maturity level methodology of the VDA ISA. For each control, a maturity level ranging from 0 to 5 ("not applicable" may also apply) is evaluated by the auditor. A TISAX label required a certain maturity level without any non-conformities (The auditee must undertake timely corrective action based on the findings and deviations from the requirements, which will be assessed in a follow-up assessment by the auditor within the specific period ).



# Contact us

**Henry Shek**

KPMG China  
Cybersecurity  
Partner  
Tel: +852 2143 8799  
henry.shek@kpmg.com

**Richard Zhang**

KPMG China  
Cybersecurity  
Partner  
Tel: +86 (21) 2212 3637  
richard.zhang@kpmg.com

**Quin Huang**

KPMG China  
Cybersecurity  
Director  
Tel: +86 (21) 2212 2355  
quin.huang@kpmg.com

**Danny Hao**

KPMG China  
Cybersecurity  
Director  
Tel: +86 (10) 8508 5498  
danny.hao@kpmg.com

**Brian Cheung**

KPMG China  
Cybersecurity  
Director  
Tel: +852 2847 5062  
brian.cheung@kpmg.com

**Frank Wu**

KPMG China  
Cybersecurity  
Associate Director  
Tel: +86 (21) 2212 3180  
fm.wu@kpmg.com

**Jason Song**

KPMG China  
Cybersecurity  
Associate Director  
Tel: +86 (21) 2212 3306  
jason.song@kpmg.com

**Jason Li**

KPMG China  
Cybersecurity  
Associate Director  
Tel: +86 (10) 8508 5497  
jz.li@kpmg.com

**John Chiu**

KPMG China  
Cybersecurity  
Associate Director  
Tel: +852 2847 5096  
john.chiu@kpmg.com

**Kevin Zhou**

KPMG China  
Cybersecurity  
Associate Director  
Tel: +86 (21) 2212 3149  
kevin.wt.zhou@kpmg.com

**Kevin Fan**

KPMG China  
Cybersecurity  
Associate Director  
Tel: +86 (21) 2212 2200  
kc.fan@kpmg.com

**Olive Wang**

KPMG China  
Cybersecurity  
Associate Director  
Tel: +86 (10) 8553 3630  
oh.wang@kpmg.com

**Andy Yuen**

KPMG China  
Cybersecurity  
Associate Director  
Tel: +852 3927 4697  
andy.yuen@kpmg.com

**William Xu**

KPMG China  
Cybersecurity  
Associate Director  
Tel: +86 (21) 2212 4633  
william.q.xu@kpmg.com

[kpmg.com/cn/socialmedia](https://kpmg.com/cn/socialmedia)



For a list of KPMG China offices, please scan the QR code or visit our website:  
<https://home.kpmg.com/cn/en/home/about/offices.html>

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2020 KPMG Huazhen LLP, a People's Republic of China partnership and KPMG Advisory (China) Limited, a limited liability company in China, are member firms of the KPMG global organisation of independent member firms affiliated with KPMG International Limited ("KPMG International"), a private English company limited by guarantee. All rights reserved. Printed in China.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.