An accreditation perspective on information security management systems (ISMS) and data protection in Germany and Mexico

GPQI
Dialogues for Innovation and Trade

Published by
Deutsche Gesellschaft für
Internationale Zusammenarbeit (GIZ) GmbH

Registered offices
Bonn and Eschborn, Germany

Global Project Quality Infrastructure
Agustín González de Cossío, No. 821
Col. del Valle Centro, 0310
Ciudad de México, México

Design
Oliver Hick-Schulz

Photo credits
Davi Costa – Unsplash, Maarten van den Heuvel – Unsplash, Maick Maciel – Unsplash, National Cancer Institute – Unsplash, Prathankarnap – Shutterstock, Public Domain Pictures – Pexels, Zapp2Photo – Shutterstock, GPQI.

On behalf of
German Federal Ministry for Economic Affairs and Climate Action (BMWK)
Berlin, Germany 2023
Mexico City, Mexico 2023

Text
Deutsche Akkreditierungsstelle GmbH (DAkkS, German National Accreditation Body)
Entidad Mexicana de Acreditación A.C.
Global Project Quality Infrastructure

The German Federal Ministry for Economic Affairs and Climate Action (BMWK) has commissioned the Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH to implement the Global Project Quality Infrastructure (GPQI).

Implemented by

Federal Ministry
for Economic Affairs
and Climate Action

giz Deutsche Gesellschaft
für Internationale
Zusammenarbeit (GIZ) GmbH

Introduction

The German-Mexican Dialogue on Quality Infrastructure is conducted between the Mexican Ministry of Economy and the German Federal Ministry for Economic Affairs and Climate Action (BMWK). Its aims are to create a political and technical dialogue platform which addresses topics of mutual interest concerning Quality Infrastructure (QI), with a view to enhancing product safety, reducing technical barriers to trade and strengthening economic exchange between the countries. On behalf of BMWK, Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH is commissioned with implementing the Global Project Quality Infrastructure (GPQI), which facilitates the dialogue.

As relevant stakeholders in the dialogue, the German National Accreditation Body (DAkkS) and Mexican Accreditation Entity (ema) held an exchange on Information Security Management Systems (ISMS) and data protection. These two fields are rapidly growing in importance on account of the increasing digitalisation of the economy.

In this brief document, the reader will gain an overview both of German and Mexican accreditation bodies and of the processes they follow to accredit certification bodies in Information Security Management Systems (ISMS) and data protection.

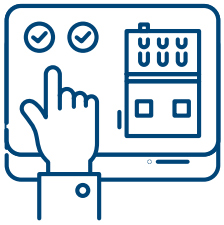
Accreditation bodies

DAkkS
Deutsche
Akkreditierungsstelle

Established in 2009, the **German National Accreditation Body** (DAkkS) fulfils the requirements of Regulation (EC) No 765/2008, being entrusted with the role of sole National Accreditation Body. DAkkS represents German accreditation interests within the national and international accreditation organisations: the International Laboratory Accreditation Cooperation (ILAC), International Accreditation Forum (IAF) and European Accreditation (EA). DAkkS is a signatory of all scopes of EA Multilateral Agreements (MLAs). Nationally, DAkkS performs the sovereign activity of assessing and supervising the competence of national conformity assessment bodies in all fields of conformity assessment. For international customers, DAkkS provides its services on a voluntary basis.

>250
employees

~4.800
accreditation certificates



~950
external assessors

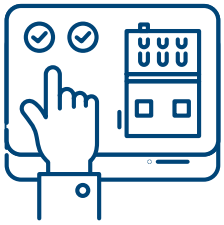
~3.900
assessments per year

The Mexican Accreditation Entity[1], (entidad mexicana de acreditación a.c., ema), was established in 1999 and carries out the evaluation and accreditation process for conformity assessment bodies in accordance with the standards applicable to each accreditation programme. It recognises laboratories offering services in Mexico according to the Good Laboratory Practices (GLP) published by the OECD.

Complying with all national and international standards relevant for accreditation, ema has been granted the highest international recognition from the International Accreditation Forum (IAF) and International Laboratory Accreditation Cooperation (ILAC), and regional recognition from the Asia Pacific Accreditation Cooperation (APAC) and Inter-American Accreditation Cooperation (IAAC).

140
employees

~6.300
accreditations



1.200
external assessors

~4.500
assessments per year

[1] In Mexico there are two further accreditation bodies: Mexicana de Acreditacion A.C. (MAAC), approved by the Ministry of Economy in 2020; and Sociedad Internacional de Accreditacion A.C. (SIAAC), approved in 2021 by the same ministry. Neither are currently involved in accreditation for ISMS or Data Protection.

Information security management systems (ISMS)

ISO/IEC 27001 is a standard for information security, which provides requirements for an information security management system (ISMS) and is thereby one of the most important certifications for cybersecurity for organisations of all types and sizes, including companies, governmental entities and non-profit organisations. Along with other standards from the ISO/IEC 27000 family, it enables organisations to manage the security of financial information, intellectual property or employee details, among other things, and offers them a tool with which to analyse, monitor and contain information security risks. **Within the framework of a more interconnected economy, having strong information security is fundamental.** ISO/IEC 27001 encompasses major data aspects such as availability, confidentiality and integrity and addresses every level of an organisation. Accreditation is a crucial step towards enhancing trust and reliability in the competence of the conformity assessment bodies that provide these certifications and other types of conformity assessments and procedures.

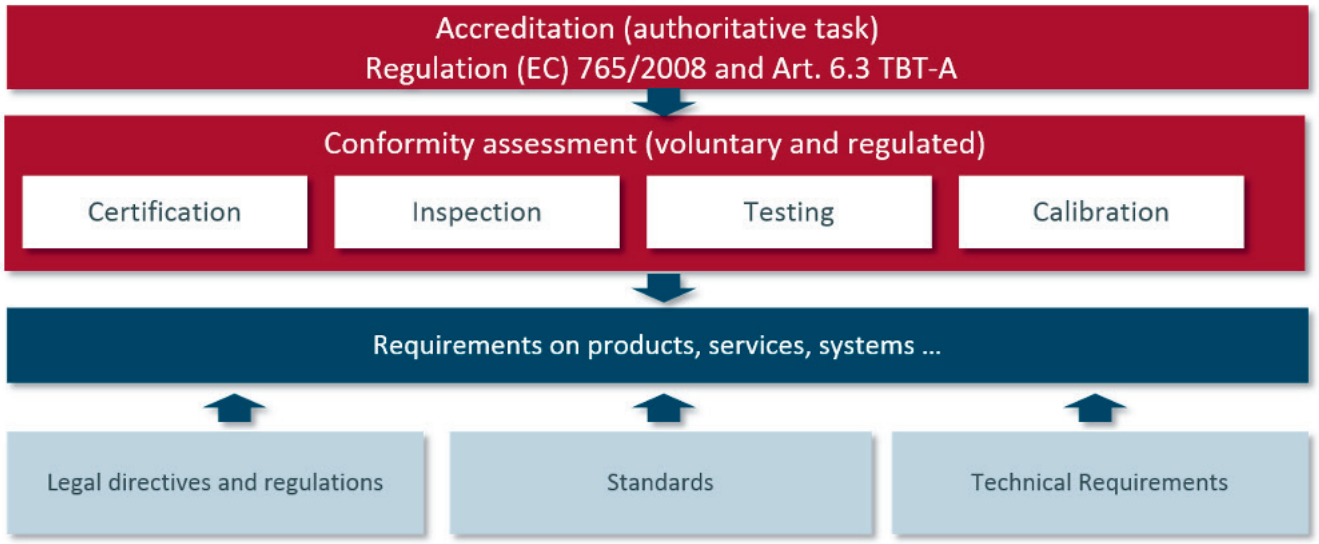
Germany

In Germany, there are currently 51 certification bodies accredited by DAkkS in line with ISO/IEC 27001 in the field of information security management systems – and the number is rising.

With regard to ISMS, DAkkS awards accreditation on the basis of ISO/IEC 17021 to a conformity assessment body, provided it fulfils the requirements set out in this harmonised international standard and potentially certain additional requirements. Additional requirements may include:

- conformity assessment programme for the accreditation of certification bodies for the IT security catalogue, in accordance with Section 11 (1b) of the Energy Industry Act (German: 'EnWG') on the basis of ISO/IEC 27006;
- Implementing Regulation (EU) 2019/1583, laying down detailed measures for the implementation of the common basic standards on aviation security, as regards cybersecurity;
- Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS).

Figure 1: The general accreditation system. Source: DAkkS



Mexico

In Mexico there are currently **13 certification bodies accredited in the field of certification of information security management systems.**

The accreditation process is based on policies established by ema as well as ISO/IEC 17021-1:2015, ISO/IEC 27001:2013, ISO/IEC 27006:2015/AMD 1:2020, among others. Mandatory documents by the IAF are additionally taken into account.
It is considered a voluntary accreditation programme by certification bodies and the industry. **Despite being an optional programme, obtaining an accredited certification gives security to end users and confidence to clients.**

Recent developments in Mexico

In recent years, Mexico has experienced a growing demand for financial services. This has encouraged entities in this sector to stay at the forefront of technological advances that promote inclusion, mobility, accessibility and cost reduction for users. This generates many benefits for the population and for the financial system, but it also entails exposure to new risks, including cyber risk. For this reason, accreditation in this field has immense potential.

The accreditation process in Germany is composed of the following steps for conformity assessment bodies:

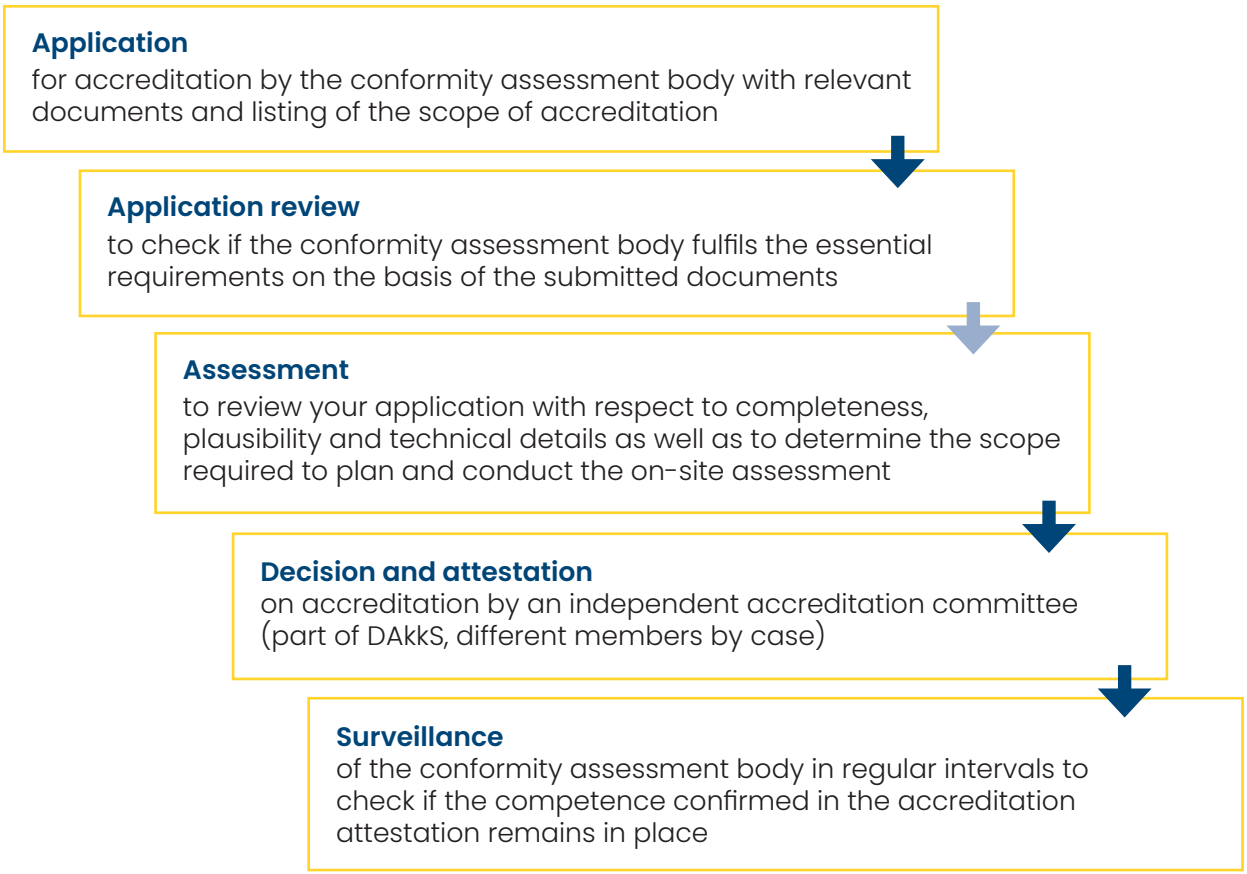


Figure 2: The accreditation process. Source: DAkkS

Data protection

Data protection focuses on protecting data and information from both internal and external threats. It mitigates the risks of fraud and corruption, while protecting the individual. As the amount of data being stored and created is continuously increasing, it has become indispensable to strengthening data protection. **To fully protect both organisations and individuals, accreditation plays a relevant role.** A brief but comprehensive summary of how it is done in Germany and Mexico is developed below.

Germany

Certification bodies seeking to confirm compliance with the **General Data Protection Regulation (GDPR)** in Germany must be accredited by DAkkS in line with ISO/IEC 17065 and approved by the data protection supervisory authority. This is regulated in Art. 43 GDPR and Art. 39 of the Federal Data Protection Act (BDSG).

The whole process, from the certification scheme review to final accreditation of the certification body, is a joint process between DAkkS and the data protection supervisory authority. In practice, this means that DAkkS performs the system assessment and the data protection supervisory authority performs the technical data protection assessment.

Currently, no certification body is accredited yet. However, four data protection certification schemes are approved and four data protection certification schemes, developed by private initiatives, are under evaluation. Within the approved schemes, certification bodies can apply for accreditation in accordance with ISO/IEC 17065 and Art. 43 of the GDPR and the supplementary requirements for accreditation of the data protection supervisory authorities.

The demand for accredited certification is immense in Germany. Nearly 50 bodies have expressed an interest in accreditation to DAkkS. The main reason for this high demand is the fact that very soon only accredited certifications will be allowed in Germany. Bodies that issue GDPR certificates without accreditation will then be prohibited by DAkkS.

Recent developments in Germany

A current hot topic is the publication of requirements for data protection certification schemes by the supervisory authorities. The publication includes application notes and test criteria for certification programmes in the field of data protection. Approval of the criteria by the supervisory authority can take place based on this publication.

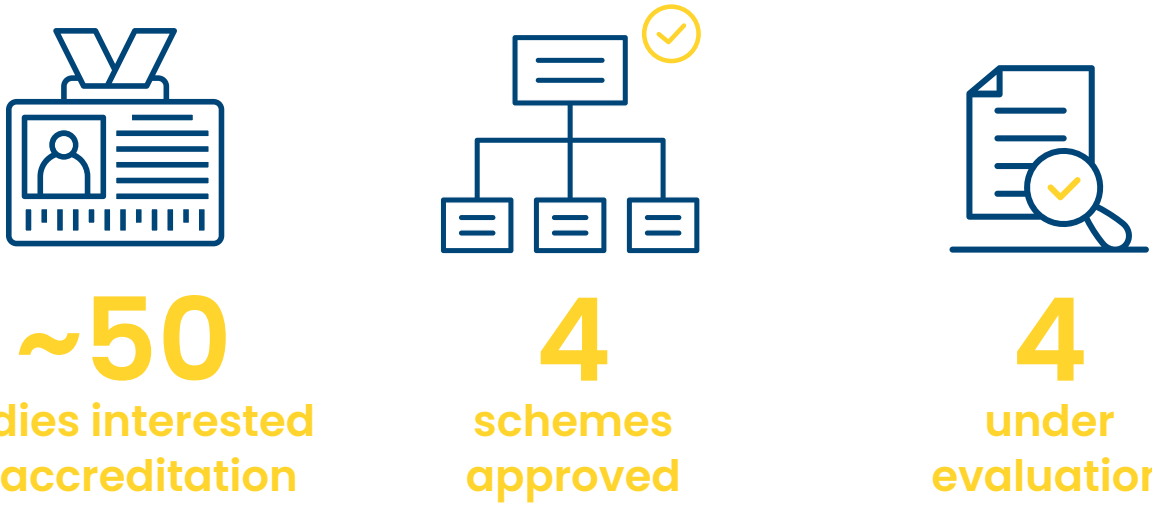


Figure 3: Data protection certification schemes. Source: DAkkS

Mexico

Under the framework of the Federal Law for the Protection of Personal Data and according to the rules of operation of the register of binding self-regulatory schemes (Chapter 3, Section 2), the National Institute of Transparency, Access to Information and Protection of Personal Data (INAI) authorises every accreditation entity. Since 2015, ema has been authorised by INAI to assess certification bodies.

While ema invites INAI representatives to participate in the assessment process, similarly – and being mindful of impartiality – INAI participates in ema's committee for accreditation decision-making.

Currently, ema has accredited two certification bodies: the Global Certification Bureau, S.A. and NYCE Sociedad Internacional de Gestión y Evaluación S.C.

Companies are obliged to certify their compliance through accredited certification bodies. Accreditation entities resolve applications for accreditation of organisations seeking to act as certification bodies in this field. They also maintain updated information on the status of the accreditations granted.

Recent developments in Mexico

On 28 January 2022, as every year, INAI celebrated a forum to commemorate the **International Day for the Protection of Personal Data.** It was organised with the collaboration of interested parties from the government and the private sector. The event is celebrated with the aim of disseminating information about and raising awareness of the importance of protecting personal data.

Learn more:

Global Project Quality Infrastructure (GPQI)
German National Accreditation Body (DAkkS)
Mexican Accreditation Entity (ema)