



How to Elevate Your Digital Trust Maturity


Actionable steps that will help you strengthen digital trust knowledge and propel your organization forwards





Measuring your level of digital trust maturity


Digital trust is key to accelerating your organization's transformation journey and building a secure, sustainable future.

Regardless of where you are in your digital trust journey, there are opportunities to strengthen capabilities, safeguard against risks, and streamline processes. That's why we've developed a digital trust maturity checklist. By completing [this checklist](#) , it will help you build organizational resilience by identifying whether your digital trust approach is at a **foundational, intermediate, or expert level**.

In this article, we explore three key elements of the digital trust maturity checklist through the three maturity levels:

- **Information security and cybersecurity**
- **Privacy management**
- **Artificial intelligence**

We'll outline the qualifications and training courses which you can leverage to help both individuals and teams in each of these areas. They will enable you to gain the necessary knowledge and skills needed to enable future growth and innovation across your organization.

Find out how mature your approach to digital trust is by using our [self-assessment checklist](#)  today.

A foundational approach >

An intermediate approach >

An expert approach >





A foundational approach to digital trust

This stage is reflective of those who are at **the beginning of their digital trust journey**. Some key attributes of foundational maturity include:

- Professionals who have an understanding of information security and privacy principles, as well as an awareness of the lifecycle of AI
- An individual within the organizations who is considered an AI, privacy, and/or cybersecurity expert
- Executives who are willing to commit time and budget to digital trust processes

To achieve this level of maturity and accelerate progress further, we recommend leveraging standards like [ISO/IEC 42001](#), [ISO/IEC 27701](#), and [ISO/IEC 27001](#). They will help you strengthen digital trust processes and implement robust frameworks.

We also suggest leveraging these training courses as they will help to solidify your knowledge and practical skills in managing Information Security, Cybersecurity, Privacy, and AI.

- [ISO/IEC 27001 Requirements](#) 
- [GDPR Foundations](#) 
- [ISO/IEC 27701 Requirements](#) 
- [ISO/IEC 22989 Understanding AI Concepts and Terminology](#) 
- NIST Cybersecurity Implementation

An intermediate approach >

An expert approach >










An intermediate approach to digital trust

At this stage of maturity, **organizations will have already implemented robust privacy and information security management controls based on industry standards.**

Key attributes of intermediate maturity include:

- **Senior leaders who have allocated adequate resources to ensure digital trust controls and processes are effectively managed**
- **Professionals across the businesses who understand the role they play in managing digital trust**
- **The development of processes regarding the responsible use of AI**

To strengthen confidence and develop the digital skills needed to responsibly harness AI potential, we recommend the following courses.

- [ISO/IEC 27001 Lead Auditor](#) 
- [ISO/IEC 24029-1:2021 - Introduction to Robustness for Neural Networks](#) 
- [BCS Certificate in Information Security Management Principles \(CISMP\)](#) 
- [IAPP Certified Information Privacy Technologist \(CIPT®\)](#) 
- [ISO/IEC 22989 Understanding AI Concepts and Terminology](#) 

A foundational approach >

An expert approach >

An expert approach to digital trust

In this final stage of maturity, **both organizations and individuals are routinely applying high standards of digital trust across all their products, services or processes.** Attributes include:

- **A culture of continuous improvement which extends across the supply chain**
- **A workforce where all employees have a robust understanding of how to harness technology like AI responsibly**
- **Demonstrable evidence that shows how Information Systems Management and cybersecurity controls are improving project delivery**

While this is currently our highest level of maturity, there are opportunities for organizations to elevate their digital trust capabilities further to prepare for the future. The solutions below will be critical for organizations who are looking to accelerate innovation and strengthen competitiveness. On an individual level, the following courses can also help you take the next step in your career and lead positive change across your organization.

[IAPP Certified Information Privacy Manager \(CIPM®\)](#)

[ISO/IEC 42001 Certified Lead Auditor Professional](#)

A foundational approach >

An intermediate approach >





Let's build a more resilient digital future together

No matter where you are in your digital trust journey, BSI's suite of solutions is designed to help you and your organization accelerate progress. All of our courses are continually updated with the latest global trends and regulatory changes and can be delivered in a way that works for you - whether it's remote, hybrid, or in person.

For more information about our digital trust training courses and qualifications, speak to our experts at visit: <https://www.bsigroup.com/th-th/forms/general-enquiry/>

Find out how mature your approach to digital trust is by using our self-assessment checklist today.

Call: **020265297**

Visit: **[bsigroup.com/th-th](https://www.bsigroup.com/th-th)**

