The dimensions of digital trust

DELVING INTO THE DEPTHS OF DIGITAL TRUST, ITS CHALLENGES, BENEFITS AND HOW WE CAN HELP

White paper

SGS.COM

SGS

Executive summary

Trust has evolved thanks to the digital age. Traditional trust has changed in an increasingly interconnected world and is no longer merely based on a person's experience and reputation.

As digitization increases and technologies evolve, establishing digital trust is essential. This white paper defines the term, its challenges and overall benefits.

Digital trust is given to organizations that prove they provide reliability, creditability, security and privacy, as well as data ethics with their online programs and devices. When a person or organization chooses an entity's product or service, they confirm their trust.

This symbiotic relationship separates dependable services from harmful ones, helping the engager differentiate between secure and insecure organizations. Digital trust creates and nurtures the bond, and assures stakeholders that the service is safe, secure and reliable.

Organizations must gain digital trust to digitally enhance themselves and customer confidence. The more digital trust an organization has, the greater the chance it will gain more users.

Consumers consider trust more than ever when purchasing a product or service, actively looking for ways to ensure they use the best sources. This is forcing organizations to examine and evolve how they function and produce services or devices with better security and reliability.

Pursuing trust is driving a digital transformation. Companies are beginning to focus on privacy management and cyber risks, and including privacy and security staff in planning and budgets.

Digital trust expedites the process of customers finding and choosing dependable digital services. Unreliable choices are falling behind.

As organizations and consumers continue to embrace cutting-edge technologies, from the internet of things (IoT) and Industry 4.0 to artificial intelligence (AI) and automation, cyber threats are evolving and becoming more frequent. They not only affect the targeted enterprise but also their business partners, suppliers and customers.

Furthermore, as consumers share more personal data online with different businesses, they are at greater risk while the importance of their confidence in the company increases.

To keep pace, organizations, individuals and nations must implement the latest protection measures to avoid hackers, data loss, lawsuits and reputational damage, among other issues. We explore innovative technologies, such as AI, alongside crucial security measures, including information security (InfoSec) and cybersecurity, to protect your organization from nefarious actors.

Finally, we summarize our Digital Trust Assurance services, including key standards and processes like business continuity. We place a key standard under the spotlight in each area – information security and cybersecurity, privacy protection, AI, business continuity and cloud security, as well as detail our other services.

Traditional trust to digital trust

Trust has evolved thanks to the digital age. Traditional trust, built on in-person interactions and personal relationships, has changed in an increasingly interconnected world.

The digital era means that trust is no longer merely based on a person's experience and reputation. The internet's relentless reviews and ratings heavily influence modern trust. Algorithms and reputation systems that determine credibility and reliability establish modern trust. Digital interactions shift how we perceive and build trust.

The speed and scale of digital transactions also challenge traditional trust. Trust must now be achieved quickly and effectively, often without human interaction. This evolution demands fresh approaches and technologies to ensure trust and security in the digital world.

Defining digital trust

As digitization increases and technologies evolve, establishing trust in the digital realm is essential. Digital trust concerns user confidence in the reliability, creditability, security and privacy of digital platforms, technologies and interactions. This trust shapes and enhances digital transactions, relationships and more.

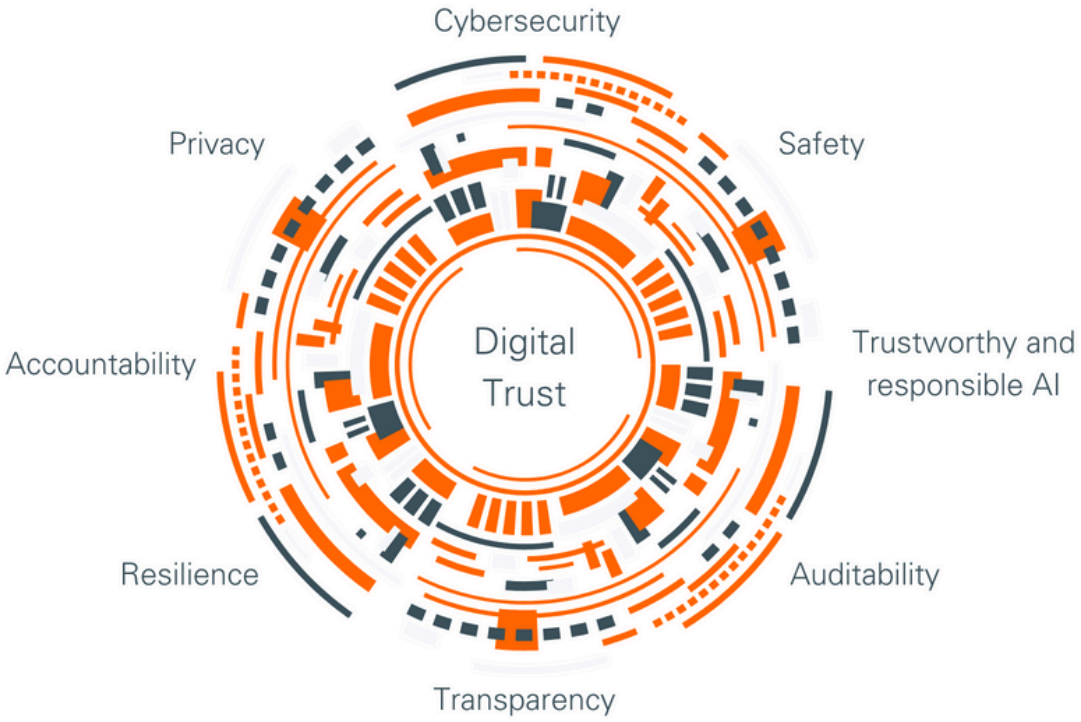
> Digital trust is the promise "that digital technologies and services – and the organizations providing them – will protect all stakeholders' interests and uphold societal expectations and values." – The World Economic Forum's Earning Digital Trust report

Defining the dimensions

Digital trust involves multiple dimensions, including:

- Reliability: the confidence that digital systems, processes and services perform consistently
- Credibility: the trustworthiness of digital information, data, sources and platforms
- Security: the protection against unsolicited access, data breaches and cyber threats that could compromise digital systems and personal data
- Privacy: the individual's control over their personal information, including how it is collected, used, stored and shared
- Identity: only authorized users and third parties should have access to business apps and data. Organizations must have identity and access management policies protecting their resources
- Predictability: implementing an effective threat-prevention and remediation strategy to anticipate possible threats and plan for cybersecurity incidents
- Risk mitigation: a key part is visibility of the status of an organization's devices. Monitoring endpoints and verifying their compliance provides insights into suitable threat-hunting practices and how to triage and detect unknown threats and vulnerabilities
- Data integrity: more than securing data, organizations must ensure that consumer data is complete, accurate and stored and handled appropriately. Data must be readily available when required
- Compliance: adherence to regulatory requirements and key industry standards, as well as building trust into business and operating models for sustainable value

SIMPLIFIED DIGITAL TRUST WHEEL



CYBERSECURITY
A framework and measures to protect against criminal/unauthorized use of data and cyberattacks.

SAFETY
A strong trust and safety framework to prevent issues, such as data breaches and fraud.

TRUSTWORTHY AND RESPONSIBLE AI
Methods to ensure AI system transparency, fairness, reliability, safety, security and accountability.

AUDITABILITY
Trace and evaluate technologies, including AI, to support strong security, privacy, data integrity and ethical behavior.

TRANSPARENCY
Clear, precise and documented operations and security. But transparency can lead to vulnerabilities.

RESILIENCE
Robust business continuity and strategies to prevent and minimize disruptions and threats.

ACCOUNTABILITY
Taking responsibility and acting to improve aspects like strategies, operations, security and more.

PRIVACY
Measures to ensure secure and transparent data handling.

A rich tapestry of relationships

Digital trust is given to organizations that prove they provide reliability, creditability, security and privacy, as well as data ethics with their online programs and devices. When a person or organization chooses an entity's product or service, they confirm their trust.

This symbiotic relationship separates dependable services from harmful ones, helping the engager differentiate between secure and insecure organizations. Digital trust creates and nurtures the bond, and assures stakeholders that the service is safe, secure and reliable.

Organizations must gain digital trust to digitally enhance themselves and customer confidence. The more digital trust an organization has, the greater the chance it will gain more users.

53% of consumers make online purchases or use digital services only after ensuring the company has a reputation for protecting customers' data.
70% in Latin and South America
65% of those buying for their organization
58% of millennials and Gen Z
– McKinsey's Why Digital Trust Truly Matters survey

Trust is transforming digitization

Consumers and, indeed, organizations consider trust more than ever when purchasing a product or service, actively looking for ways to ensure they use the best sources. This is forcing organizations to examine and evolve how they function and produce services or devices with better security and reliability.

Pursuing trust is driving a digital transformation. Companies are beginning to focus on privacy management and cyber risks, and including privacy and security staff in planning and budgets.

Digital trust expedites the process of customers finding and choosing dependable digital services. Unreliable choices are falling behind. Eventually, machines will automate this decision-making process by determining an entity, product or service's confidence level. This will involve more information regarding an organization, its product or service, creating greater transparency and digital trust.

Factors important in the buying decision (% of respondents)
Price – 94%
Description – 93%
Quality – 92%
Convenience – 92%
Ethical and trusted reputation – 87%
Amount of personal data required – 87%
Speed of delivery – 87%
– McKinsey's Why Digital Trust Truly Matters survey

Digital identity and trust

Digital identity is vital to establishing trust in the digital sphere. Digital identities foster trust between people, organizations and digital platforms. They are a way to confirm user identity, ensuring secure and reliable interactions and transactions.

Identity verification technologies, including multi-factor authentication and biometrics, add layers of security and assurance to enhance digital trust.

Digital trust and the internet of things (IoT)

IoT technologies have vulnerabilities across every industry. Consumers are losing confidence in manufacturers' abilities to produce safe and secure products. Such devices are often built without considering security, exposing them to hackers and data breaches. Organizations are losing digital trust in them.

Without trust, IoT will not achieve its intended outcomes. To cultivate trust, IoT device manufacturers must initially focus on device authentication process security improvements. Digital trust cannot happen if the device lacks a robust authentication method that protects users from malware. IoT must protect personal, sensitive data shared on devices through encryption.

The role of the tech sector

As modern technologies, such as AI, transform virtually all industries and economies, the question of how to benefit and adopt them responsibly is raised.

The World Economic Forum (WEF) is actively engaging over 100 companies, from numerous industries, to support responsible AI adoption, as part of its AI Governance Alliance. This came about because companies have a multitude of reasons to get this right, including economic and potential liability if AI leads to adverse outcomes.

Digital trust as a pathway to risk mitigation

Digital trust is inspiring organizations to focus on mitigating risk because the failure to adequately manage risk negatively impacts consumer confidence levels.

Business leaders are now including information security, cybersecurity and privacy protection, among other security aspects, in the development process. This helps ensure that the business does not avoid security measures just to get their device or service to market.

Some organizations are also adopting a zero-trust model, which limits privileged access to different systems or network segments, to reduce the opportunities a hacker has to swipe secure content.

Technology-enabled digital trust

As organizations and consumers continue to embrace cutting-edge technologies, from IoT and Industry 4.0 to AI and automation, cyber threats are evolving and becoming more frequent. They not only affect the targeted enterprise but also their business partners, suppliers and customers.

Furthermore, as consumers share more personal data online with different businesses, they are at greater risk while the importance of their confidence in the company increases.

To keep pace, organizations, individuals and nations must implement the latest protection measures to avoid hackers, data loss, lawsuits and reputational damage, among other issues.

BLOCKCHAIN

This decentralized, encrypted technology ensures the integrity of digital records. Blockchain enables trust in transactions by eliminating the reliance on intermediaries and ensuring transparency and immutability.

ARTIFICIAL INTELLIGENCE (AI)

AI can promote digital trust. Certain AI-powered systems can analyze enormous amounts of data and identify anomalies and potential threats, enhancing security and trust.

72% of respondents said that knowing a company's AI policies is important before making a purchase.
– McKinsey's Why Digital Trust Truly Matters survey

Security- and safety-enabled digital trust

INFORMATION SECURITY AND CYBERSECURITY

Information security (InfoSec) and cybersecurity safeguard an organization's digital data. They prevent unauthorized access, damage or editing, and guard against cyberattacks targeting sensitive information, blackmail or business interference, through various processes, tools and technologies.

Technologies, such as encryption, firewalls and intrusion-detection devices, coupled with staff updated on the latest threats and protection measures, will significantly help protect data and systems against unauthorized access, strengthening trust in digital interactions.

PRIVACY PROTECTION

85% of respondents said that knowing a company's data privacy policies is important before making a purchase.
– McKinsey's Why Digital Trust Truly Matters survey

Privacy protection ensures that an organization collects, uses and secures personal data through policies and technologies to prevent data from being unlawfully accessed, modified or disclosed. It also involves legal and ethical considerations to safeguard the individual's right to privacy.

Trust is created and enhanced if thorough, end-to-end privacy protection exists and is indicated.

CRUCIAL SECURITY BEST PRACTICES

Key security best practices include:

- Utilize automated tools to prevent cyber threats, enhance security and decrease overheads
- Deploy active defenses against cyber threats, including endpoint malware-prevention solutions
- Implement data storage and access policies
- Obtain key certifications, such as:
  - ISO/IEC 27001 (information security, cybersecurity and privacy protection)
  - ISO/IEC 27701 (privacy information management system, or PIMS)
  - ISO/IEC 42001 (AI management system)
- Install an incident-response program and test regularly
- Meticulously assess privacy risks when using external data
- Implement procedures to handle data privacy breaches
- Integrate security considerations when designing new technology

BUSINESS CONTINUITY

Business continuity enables an organization to maintain critical business functions during and after a disaster.

This action ultimately creates trust through reliability and credibility, and security if the associated systems are maintained.

Why digital trust truly matters

Digital trust creates many advantages for companies, including:

- A positive and enhanced reputation among customers and stakeholders
- Fewer cybersecurity incidents and privacy breaches that can destroy credibility and assets
- More reliable data for decision-making that can improve performance and innovation
- Stronger customer loyalty that can increase revenue and retention
- Faster innovation due to confidence in technologies and systems that can enhance competitiveness and growth

The McKinsey Why Digital Trust Truly Matters showed that:

- 46% of consumers often or always consider another brand if the one they are considering purchasing from is unclear about how it will use their data
  - 58% of Asia-pacific respondents
  - 56% of those buying for their organization
  - 50%+ of millennials and Gen Z respondents
- 53% of customers would only buy from companies with a reputation of protecting customer data. This is 65% for those buying for their organization
- 40% of consumers would cease business with a company after learning their data was not protected
- 10% of customers would stop working with companies after a data breach, even if their data was unaffected

Entrust us with your digital trust

Our Digital Trust Assurance services enable you to meet the latest standards, from ISO/IEC 27001 (information security, cybersecurity and privacy protection) to ISO/IEC 42001 (AI management system), enhancing your service, security and brand.

Combining decades of digital expertise worldwide with the latest knowledge of trends and technologies, we support your digitization, security implementation, business continuity and supply chain security – whatever your business type, size and location.

We enable you to:

- Assess information security across your organization
- Meet and exceed cybersecurity thresholds
- Embrace AI quickly and safely
- Deliver precise privacy protection, handling and storing the correct data securely
- Ensure business continuity, especially during high-risk situations
- Plan, implement and minimize risk when adopting advanced technologies
- Strategize and deploy optimal security measures
- Comply with key international, national and local legislation and regulations

Information security and cybersecurity services

Information security and cybersecurity safeguard your digital and physical data. They prevent unauthorized access, alteration or damage, and protect against hackers targeting sensitive information, extortion or business disruption, through a range of processes, tools and technologies.

Our digital expertise and essential services, such as ISO/IEC 27001 certification for information security, cybersecurity and privacy protection, enhance security and shield your systems, devices, applications and sensitive data.

UNDER THE SPOTLIGHT: ISO/IEC 27001

A robust information security management system (ISMS) enables you to exploit interconnectivity while managing information security, cybersecurity and privacy risks.

ISO/IEC 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an ISMS. It also sets out the requirements for assessing and treating cyber risks, based on your specific needs.

Achieving certification demonstrates your commitment to information security and assures clients and other partners that you are serious about protecting information under your control.

What are the benefits of certification?

ISO/IEC 27001 certification follows successful completion of an audit. The long-term benefits include:

- Enhanced credibility
- Reduced risk of fraud, information loss and disclosure
- Demonstration of integrity to your system
- Business culture transformation and greater awareness of the importance of keeping information secure
- New business opportunities with security-conscious customers
- A stronger notion of confidentiality throughout the workplace
- Better preparedness for the unavoidable – the next security event or incident

Privacy protection services

Privacy protection ensures that you collect, use and secure personal data through policies and technologies to prevent data from being unlawfully accessed, modified or disclosed. It also involves legal and ethical considerations to safeguard the individual's right to privacy.

Through our extensive expert support and services, including ISO/IEC 27701 (privacy information management system, or PIMS) and Europrivacy certification, you can achieve precise privacy protection and comply with key regulations.

UNDER THE SPOTLIGHT: EUROPRIVACY

Europrivacy provides a comprehensive set of online resources and services to help you effectively implement, enhance and demonstrate compliance with the General Data Protection Regulation (GDPR) and complementary data protection regulations. The European Data Protection Board (EDPB) approved Europrivacy as the European Data Protection Seal.

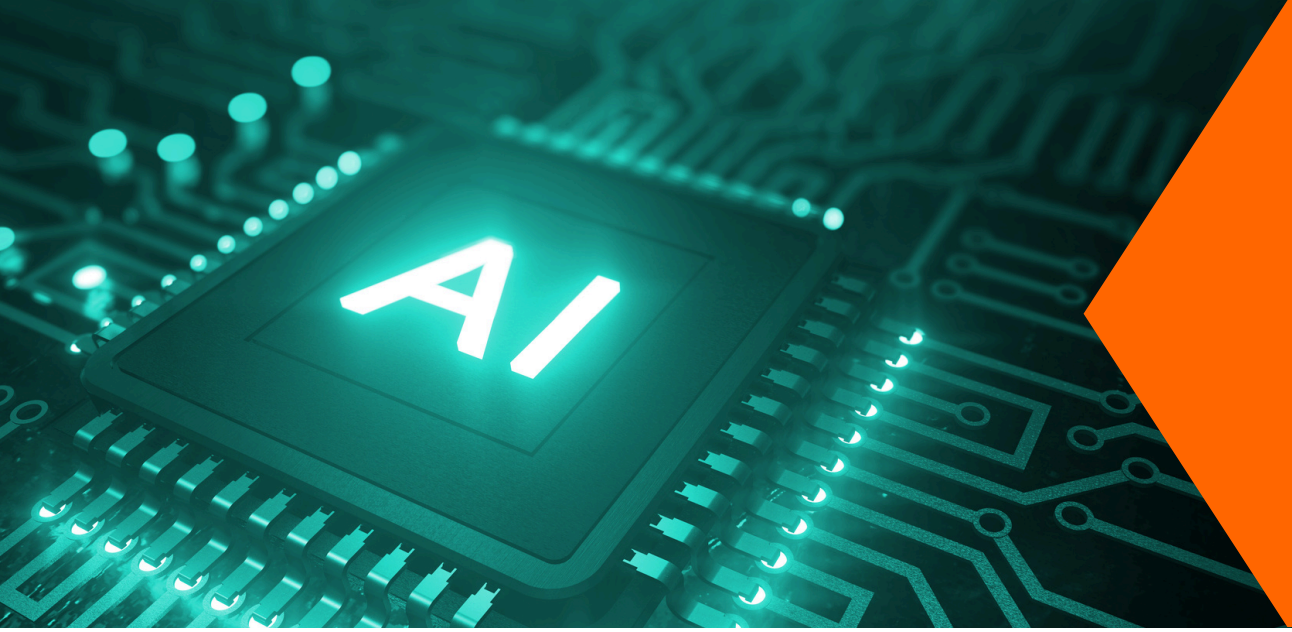
Adopting a hybrid model, Europrivacy applies to almost all data processing activities, including emerging technologies like AI, blockchain and IoT.

The scheme can enable applicants to identify and reduce risks, demonstrate and value compliance, and enhance reputation and market access. It is the only GDPR certification to be officially recognized in all EU member states.

What are the benefits of certification?

Europrivacy enables you to:

- Identify and reduce the legal and financial risks of noncompliance
- Document, assess, certify, value, communicate, maintain and enhance compliance
- Build trust and confidence among data subjects, B2B partners and stakeholders
- Develop competitive advantages
- Improve reputation and market access
- Increase market valuation by reducing risks and uncertainty for investors
- Save time and cost thanks to Europrivacy's innovative methodology
- Support cross-border and processor data transfers
- Reduce risks and costs with data processors
- Extend compliance assessment to non-EU jurisdictions
- Join a business ecosystem committed to data protection



AI services

AI is revolutionizing modern life and business at an astonishing pace by enabling computers to learn and solve problems like humans. By learning patterns and structures in vast datasets, it can perform a range of tasks, from predicting consumer product preferences to engaging in human-like conversations.

Combining our vast digital trust expertise, we help you understand, apply and enhance AI systems safely through vital services like ISO/IEC 42001 (AI management system, or AIMS) certification.

Top 10 AI predictions for 2025

1. AI-augmented workspace
2. Advanced voice assistants
3. Sustainable AI
4. AI in cybersecurity
5. Quantum AI
6. AI legislation and regulation
7. Generative video AI
8. Responsible AI
9. Agentic AI
10. AI in healthcare

– Compiled by AI Magazine

UNDER THE SPOTLIGHT: ISO/IEC 42001

Responding to the rise of AI and the challenges it creates, the ISO and IEC created the ISO/IEC 42001 standard. It provides a certifiable AIMS framework in which AI systems can be developed and deployed as part of an AI assurance ecosystem.

The global standard specifies the requirements for establishing, implementing, maintaining and continually improving an AIMS. The goal is to help organizations and society benefit the most from AI while reassuring stakeholders that systems are being developed and used responsibly.

What are the benefits of certification?

ISO/IEC 42001 certification follows successful completion of an audit and enables you to:

- Implement AI safely, with evidence of responsibility and accountability
- Consider security, safety, fairness, transparency and data and AI system quality throughout the life cycle
- Show that introducing AI is a strategic decision with clear objectives
- Indicate strong governance concerning AI
- Strike a balance between governance and innovation
- Ensure that AI is used responsibly, especially concerning its continuous learning
- Ensure that all relevant safeguards are in place
- Combine key frameworks with experience to implement crucial processes like risk, life cycle and data quality management

Business continuity services

Business continuity enables your organization to maintain critical business functions during and after a disaster. As a result, you should execute a business continuity plan with robust risk management processes that can prevent mission-critical service disruption and reestablish full day-to-day functions as efficiently as possible.

Our business continuity services enable you to consider unpredictable events and potential threats, such as cyberattacks, supply chain disruptions, natural disasters, disease outbreaks and other external issues.

Our experts and services, including the principal business continuity standard – ISO 22301 – enable you to keep your organization going during and after interruptions to maintain profitability, customer satisfaction, worker well-being and sustainability.

UNDER THE SPOTLIGHT: ISO 22301

Every organization will need to respond to an incident that disrupts daily business operations. Therefore, a successful business continuity management system (BCMS) is essential.

The standard specifies the requirements for implementing, maintaining and improving a BCMS to protect against, reduce the impact of, respond to and recover from disruptions.

What are the benefits of certification?

ISO 22301 certification follows successful completion of an audit and enables you to:

- Implement organization-wide identification and understanding of critical business processes and the impact of disruptions
- Proactively minimize impact
- Increase resilience levels and recovery capabilities, as well as ensure that the business survives
- Minimize downtime during incidents and improve recovery time(s)
- Gain an advantage over less resilient competitors
- Demonstrate resilience to customers, suppliers, media and stakeholders, especially during crisis conditions

Cloud security services

Cloud computing is crucial for advanced agility, flexibility, innovation and meeting consumer expectations. To ensure a secure cloud environment, effective cloud security implementation is vital.

Our cloud security services incorporate cybersecurity policies, best practices, controls and technologies that secure your cloud's data, apps and infrastructure.

We enable you to ensure storage and protection against internal and external threats, access management, data governance and compliance, and incident relief.

From support with ISO/IEC 27017 (information security for cloud services) and ISO/IEC 27018 (personally identifiable information in public clouds) to Cloud Security Alliance Security, Trust, Assurance and Risk (CSA STAR), our years of digital expertise will raise your cloud game.

UNDER THE SPOTLIGHT: CSA STAR

CSA STAR helps your organization provide or use cloud services by promoting greater transparency and shared responsibility.

Certification involves a rigorous, independent, third-party assessment of the security posture. Cloud service providers (CSPs) and customers can demonstrate adherence to this well-established, globally recognized security control specific to cloud services. It is based on achieving ISO/IEC 27001 certification and Cloud Controls Matrix (CCM) criteria.

CSA STAR certification also demonstrates that applicable cloud security issues have been assessed against the STAR Capability Maturity Model for managing activities in CCM control areas.

Alongside an existing ISO/IEC 27001 certificate, CSA STAR certification provides evidence of an actively managed cloud security program.

What are the benefits of certification?

Certification follows successful completion of an audit. The long-term benefits include:

- Industry-recognized, third-party certification based on the CSA requirements catalog
- Create more confidence, reputation and business as customers ask for proof of cloud security measures
- Provide top management with visibility to evaluate their management system relating to cloud security industry expectations and ISO/IEC 27001
- Showcase how your organization aims to optimize cloud services
- Demonstrate progress and performance through an independently validated award from an external certified body
- Benchmark performance against your peers

Digital trust advisory services

Using cutting-edge technologies, such as IoT, Industry 4.0 and blockchain, presents significant challenges, including cybersecurity threats and regulatory fines. Identifying the ideal technologies for your business and understanding their associated risks are crucial for seamless digital transformation, trust and optimal results.

With extensive experience in the digital domain, our specialist consultants guide you through your digital trust journey. We help you harness the appropriate technologies and manage the necessary data to boost business efficiency and continuity. Our expertise ensures robust security, cost reduction, faster deployment, peace of mind and more.

Digital trust training

Organizations deal with a lot of sensitive data about themselves, their customers and their stakeholders. Knowing what to store and how to protect it is essential. From information security and cybersecurity to privacy protection and automotive industry systems, we have a course to help you ensure best practices and regulatory requirements.

Supply chain digital and IT security services

Digitizing your supply chain enhances efficiency through technologies, such as AI, blockchain and cloud computing, eliminating manual processes and fostering a real-time, interconnected ecosystem.

Supply Chain 4.0 and digital twins optimize operations and predict outcomes, significantly improving decision-making. However, these advancements also increase the risk of cyberattacks and information security breaches, highlighting the need for robust safeguards.

Combining decades in the digital arena with world-leading customized supply chain audits, mapping, management and more, we support your digital supply chain and IT journey to ensure the most effective security measures.

Begin to boost your digital trust

Contact our experts now to determine your digital needs and reinforce your protective measures.

For more information:
Digital Trust Assurance section on www.sgs.com
Certification@sgs.com

References

AI Magazine – https://aimagazine.com/articles/top-10-ai-predictions-for-2025

Engati – https://www.engati.com/blog/what-is-digital-trust-and-why-its-important

IBM – https://www.ibm.com/think/topics/information-security

ISACA – https://www.isaca.org/about-us/newsroom/press-releases/2022/new-digital-trust-research-reveals-gaps-benefits-and-key-takeaways

Jamf – https://www.jamf.com/blog/digital-trust-5-reasons-it-matters-for-your-business/

McKinsey – https://www.mckinsey.com/capabilities/quantumblack/our-insights/why-digital-trust-truly-matters

Medium – https://medium.com/digital-trust-iq/what-is-digital-trust-c7a85d1163fd

Security Magazine – https://www.securitymagazine.com/articles/98355-the-benefits-of-digital-trust

SGS – https://www.sgs.com/en

SGS Digital Trust Assurance – https://www.sgs.com/en/our-services/business-assurance/digital-trust-assurance

TechTarget – https://www.techtarget.com/whatis/definition/digital-trust

World Economic Forum (WEF) – https://www.weforum.org/stories/2024/11/explainer-what-is-digital-trust-in-the-intelligent-age/

When you need to be sure

SGS Headquarters
1 Place des Alpes
P.O. Box 2152
1211 Geneva 1
Switzerland

sgs.com