






# CyberMatterz

UNIFIED ADVERSARY SERVICES



 [www.cybermatterz.com](http://www.cybermatterz.com)

 [info@cybermatterz.com](mailto:info@cybermatterz.com)

 +61 493 692 944

We are dedicated to finding innovative and cost-effective solutions and ensuring complete client satisfaction upon delivery. We strive to be genuine consulting and audit partners, refraining from hardware/software sales to ensure unbiased views and recommendations. We provide industry-specific insight and relevant recommendations to help you achieve your quality goals. We will send you documents that detail the analysis process, findings supported by evidence, and detailed recommendations.





# LOCKING OUT THREATS, UNLOCKING POTENTIAL



## OUR VISION



A connected ecosystem where international collaboration and information sharing are paramount, fostering a united front against cyber threats and creating a collective defense posture.



Our company is at the forefront of cybersecurity innovation, driving advancements that anticipate and counter emerging threats, setting industry standards, and shaping the future of digital security.



We aspire to be the trusted advisor for our clients, offering not only cutting edge cybersecurity solutions but also strategic guidance that aligns with their unique challenges and goals.

## OUR MISSION



We are committed to delivering cutting edge cybersecurity solutions that safeguard sensitive information, protect digital assets, and ensure the privacy and integrity of our clients. We strive to stay ahead of evolving cyber threats through advanced cybersecurity technologies.



Through relentless innovation, expert analysis, and a dedication to excellence, we strive to be the trusted partner in cybersecurity, enabling our clients to embrace the opportunities of the digital world while mitigating the evolving risks. We operate with the highest ethical standards, ensuring the confidentiality, integrity, and availability of our clients' digital assets.

## WHY CHOOSE US?

With a team of seasoned cybersecurity professionals, we bring years of collective experience in safeguarding organizations against a constantly evolving threat landscape. Our experts stay ahead of emerging risks to provide you with proactive and effective solutions.



We recognize the responsibility we bear in protecting the digital infrastructure. Our goal is to minimize the impact of cyber threats, contribute to a safer online ecosystem, and ensure the long-term sustainability of digital trust. By working closely with our clients, industry peers, and cybersecurity experts, we enhance our collective ability to combat cyber threats.



## OUR SERVICES



### COMPLIANCE AND GOVERNANCE

Our services will help you standardize and automate security within your processes by assessing proper data authorization, authentication, data encryption methods, password management, backup and recovery process review, support, and by optimizing internal training programs.



### IT AUDIT AND ADVISORY

We are dedicated to assisting organizations in protecting their data and technology infrastructure while also mitigating risk. We take a proactive approach in monitoring client network environment(s) and providing regulatory compliance. We have partnerships with some of the most trusted companies and institutions in the security sector.



### VULNERABILITY MANAGEMENT

Identify, contextualize, and validate vulnerabilities and assist in prioritization, remediation, and mitigation of exposure. We provide a holistic approach to managing vulnerability risks to uncover weaknesses in your organization. Our threat-centric approach to vulnerability management helps provide organizations with an accurate view of risk exposure.





## WEB APP SECURITY ASSESSMENT

A Web Application Security Assessment is a cybersecurity practice specifically tailored to test web-based service applications. This assessment aims to determine whether an application is secure and complies with standard security requirements. It validates whether the web application is designed and configured in alignment with security best practices.

---



## MOBILE SECURITY RISK ASSESSMENT

It is an evaluation process that analyzes the security risks associated with Mobile Devices, Mobile Applications, and Mobile Infrastructure. This assessment is designed to identify vulnerabilities and threats posed by various attackers, including malicious users, external and internal attackers seeking to exploit weaknesses in mobile devices and infrastructure.

---



## SECURE CONFIGURATION ASSESSMENT

Assessing risks prevalent within an organization's systems and network is crucial. This is precisely why a secure configuration assessment is conducted. The assessment provides a comprehensive analysis of potential vulnerabilities and misconfigurations in systems and applications. This includes scanning operating systems, networks, and databases.

---



## VIRTUALIZATION RISK ASSESSMENT

It involves an evaluation process designed to help identify and mitigate risks to your virtual infrastructure. This assessment encompasses a review of critical components, including people, processes, and technology that are integral to the virtual infrastructure. The reports and findings from this assessment provide a detailed list of security vulnerabilities and gaps in the system.

# ISO 9001:2015 ADVISORY AND CERTIFICATION



ISO 9001 Certification is a globally recognized and accepted Quality Management Standard developed in collaboration with the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It is a strong framework that allows organizations to demonstrate their high-level quality and risk management strategies, which are industry best practices.

## ISO 9001 Benefits



## How does ISO 9001 works?

ISO 9001 certification is not a one-time achievement; it requires ongoing commitment to quality management principles. The benefits include improved customer satisfaction, enhanced operational efficiency, and a competitive edge in the market.

The organization establishes a quality policy, outlining its commitment to meeting customer requirements and continuously improving its processes. Quality objectives are then set to drive improvement efforts. Identification and mapping of key processes within the organization. This includes processes for product realization, resource management, measurement, analysis, and improvement.

## Cyber Matterz Approaches to ISO 9001

### Initial Study

Begin with an initial business analysis to grasp the intricacies of your card processes and the surrounding environment.

### Scope Definition

Gain insight into your company's functions, controls, and systems to delineate the necessary scope.

### Gap Analysis

Evaluate your organization against the ISO9001 standard to pinpoint areas that demand focus.

### Awareness Training

Provide a concise ISO 9001 Awareness Training session for organization. Increase awareness among employees about the importance of risk management.

### Asset Classification

Recognize your vital information assets and categorize them accordingly, establishing a distinct inventory of assets.

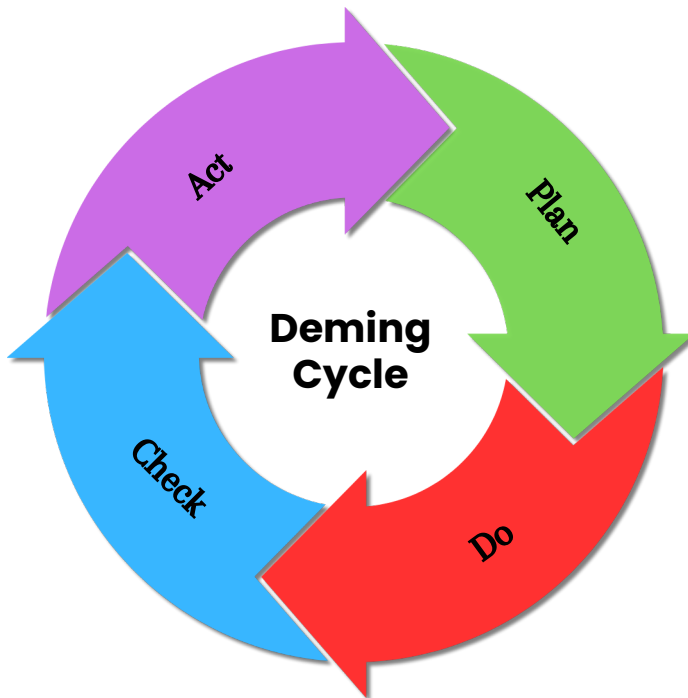
### Risk Assessment

Undertake a comprehensive risk assessment to uncover vulnerabilities and deficiencies that may pose a threat to your business.

# ISO 14001 ENVIRONMENTAL MANAGEMENT SYSTEMS

ISO 14001 is an international standard for environmental management systems (EMS). It provides a framework for organizations to establish, implement, maintain, and continually improve an effective environmental management system. ISO 14001 is designed to help organizations manage and reduce their environmental impact, comply with regulations, and achieve environmental objectives.

## ISO 14001 Methodology

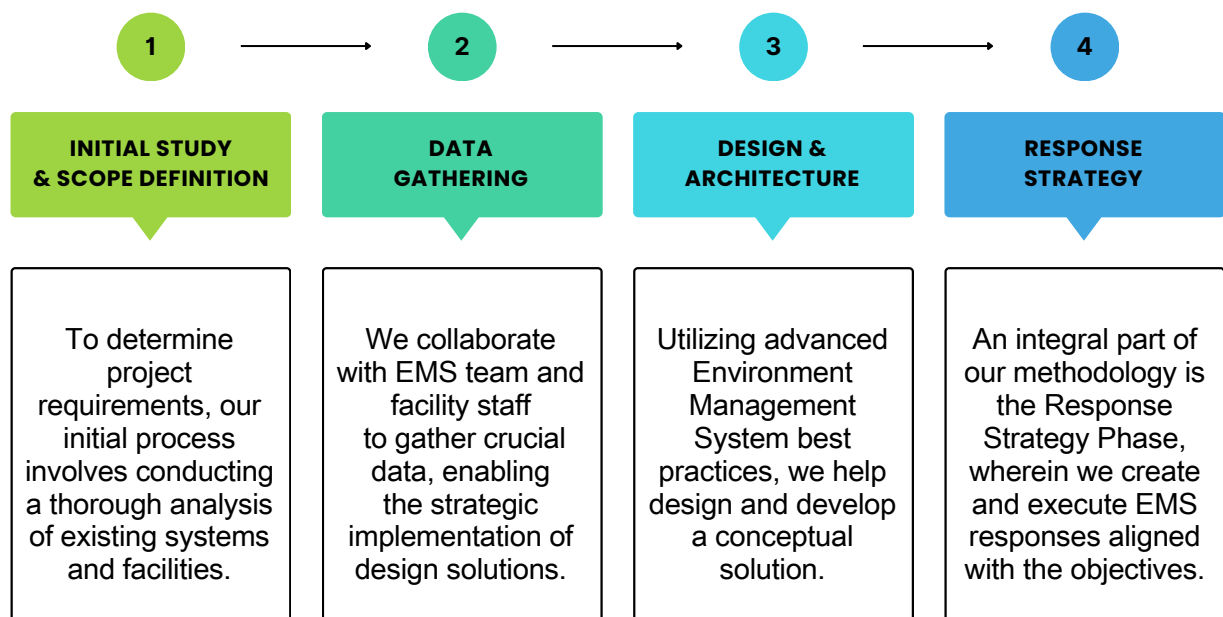


## How does ISO 14001 works?

ISO 14001 is to help organizations establish, implement, maintain, and continually improve an environmental management system, providing a framework for managing environmental responsibilities in a systematic manner.

The organization strives for continual improvement of its environmental management system by taking corrective actions to address nonconformities and preventive actions to prevent potential issues. ISO 14001 provides a systematic approach to environmental management, helping organizations identify and manage their environmental impacts while demonstrating a commitment to sustainability.

## Cyber Matterz approaches to ISO 14001



# ISO 22301 BUSINESS CONTINUITY

Business Continuity Management involves creating a strategy to prevent and recover from unexpected events such as fires, floods, or cyber-attacks. The process includes establishing detailed procedures and instructions for organizations to follow in case of a disaster. This requires identifying all potential risks that could affect business operations. The goal is to help organizations sustain their operations during significant events or disasters.

## How does ISO 22301 works?



## ISO 22301 Benefits

ISO 22301 helps organizations identify and prioritize critical business functions, ensuring that plans are in place to maintain or quickly restore them in the face of disruptions. This enhances the organization's overall resilience to unexpected events.

ISO 22301 encourages organizations to identify and assess potential risks that could disrupt business operations. By understanding these risks, organizations can develop strategies to mitigate them and be better prepared for unforeseen events. It emphasizes the importance of having effective communication and decision-making processes during disruptions. This ensures that key stakeholders are informed, and decisions can be made promptly to manage and mitigate the impact of disruptions.

## Cyber Matterz approaches to ISO 22301

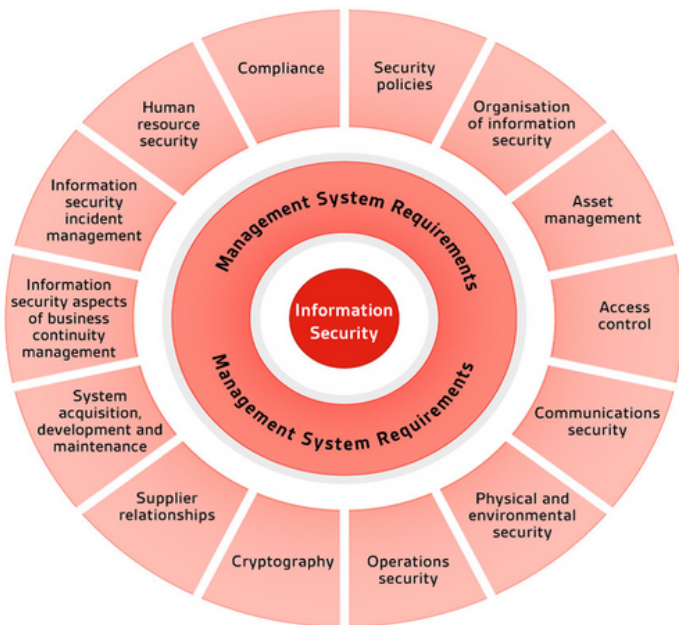




# ISO 27001 ADVISORY AND CERTIFICATION

ISO 27001 Certification is a globally recognized and accepted Information Security Standard developed in collaboration with the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). It is a strong framework that allows organizations to demonstrate their high-level security and risk management strategies, which are industry best practices.

## ISO 27001 Requirements



## ISO 27001 Benefits

Protect your data, wherever it is  
Protect all forms of information, whether digital, hard copy or in the Cloud.

Reduce information security costs  
Implement only the security controls you need, helping you get the most from your budget.

Improve company culture  
An ISMS encompasses people, processes and technology, ensuring staff understand risks and embrace security as part of their everyday working practices.

## How to achieve ISO 27001 compliance

- Scoping the project.
- Securing management commitment and budget.
- Identifying interested parties and legal, regulatory and contractual requirements.
- Conducting a risk assessment.
- Reviewing and implementing the required controls.
- Developing internal competence to manage the project.
- Developing the appropriate documentation.
- Conducting staff awareness training.

## How does ISO 27001 works?

ISO 27001 focuses on protecting the Confidentiality, Integrity, and Availability of business information or data, which may include customer data, employee information, financial information, intellectual property, or information entrusted to third parties.

It places a strong emphasis on the establishment and maintenance of an ISMS. This system is a framework of policies, processes, risk management practices, and controls designed to protect the confidentiality, integrity, and availability of information. Organizations are expected to select and implement the controls based on their risk assessment.



# ISO 20000 ADVISORY AND CERTIFICATION

The Datacenter Service offers a comprehensive approach to safeguarding your company's vital IT infrastructure. This inclusive service includes an initial assessment, strategy development, design assistance, implementation support, and ongoing operational services. Cyber Matterz, uniquely positioned in the industry, provides exceptional critical facility services with experienced datacenter designers and expert analysts.

## ISO 20000 Methodology



## ISO 20000 Benefits

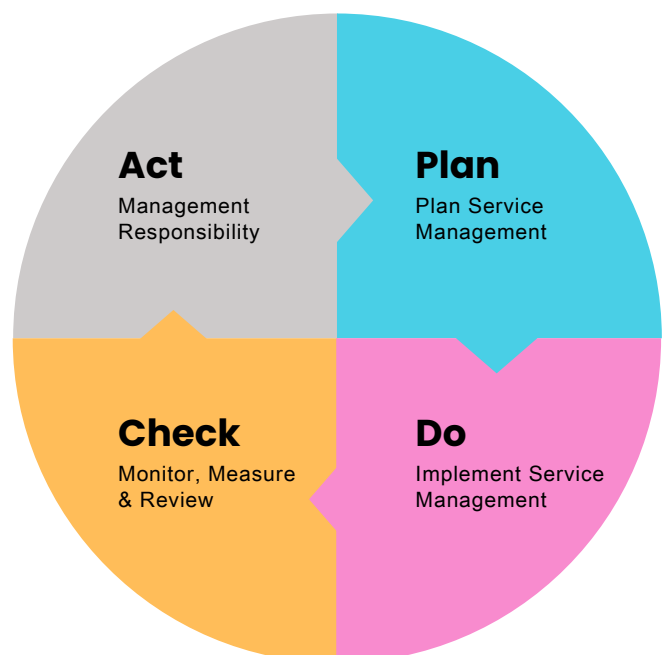
ISO 20000 provides a framework for organizations to define and implement processes that contribute to the delivery of high-quality IT services. This can lead to improved customer satisfaction and confidence in the organization's IT services.

ISO 20000 emphasizes the importance of data-driven decision-making through the use of performance metrics and key performance indicators (KPIs). It requires organizations to align IT services with business objectives. The standard encourages the adoption of efficient and effective IT service management practices, leading to cost savings and resource optimization. Well-defined processes and procedures can reduce waste and enhance the overall efficiency of IT service delivery.

## Who can ISO 20000 be used by?



- Organizations seeking services from service providers and requiring assurance that their service requirements will be fulfilled.
- An organization that requires a consistent approach by all its service providers, including those in a supply chain.
- A service provider that intends to demonstrate its capability for the design, transition, delivery, and improvement of services that fulfill service requirements.
- Service provider to monitor, measure and review its service management processes and services.



# ISO 31000 ADVISORY AND CERTIFICATION

ISO 31000 is an international standard that provides guidelines for risk management. It is applicable to any organization, regardless of its size, industry, or sector. ISO 31000 aims to help organizations establish a systematic and effective approach to risk management, considering both potential opportunities and adverse effects.

## ISO 31000 Framework



## ISO 31000 Benefits

ISO 31000 helps organizations make informed and effective decisions by systematically identifying, assessing, and managing risks. This contributes to better decision-making at all levels of the organization.

ISO 31000 helps organizations enhance their resilience to unforeseen events and disruptions. The systematic approach to risk management ensures that organizations are better prepared to respond to and recover from adverse situations.

ISO 31000 supports better governance by integrating risk management into decision-making processes. It also helps organizations ensure compliance with legal and regulatory requirements related to risk management.

## How to implement ISO 31000

- Leadership and Commitment
- Integration with Organizational Context
- Risk Management Framework
- Risk Identification
- Monitoring and Review
- Communication and Consultation
- Integration with Organizational Processes
- Documentation and Record Keeping
- Training and Awareness
- Regular Audits and Reviews
- Continuous Improvement

## How does ISO 31000 works?

Organizations begin by establishing the context for risk management. This involves understanding the internal and external factors that may influence the achievement of objectives.

Continuously monitor and review the effectiveness of the risk management process. Review the organization's risk management performance and the effectiveness of risk treatments.

Implement training programs to ensure that personnel understand their roles and responsibilities. It provide training on risk management concepts and methodologies.



# ISO 45001 OCCUPATIONAL HEALTH AND SAFETY MANAGEMENT SYSTEMS

ISO 45001 is an international standard for occupational health and safety management systems (OH&S). It provides a framework for organizations to establish, implement, maintain, and continually improve an effective occupational health and safety management system. ISO 45001 is designed to help organizations ensure the health and safety of workers, prevent work-related injuries and illnesses, and comply with applicable legal requirements.

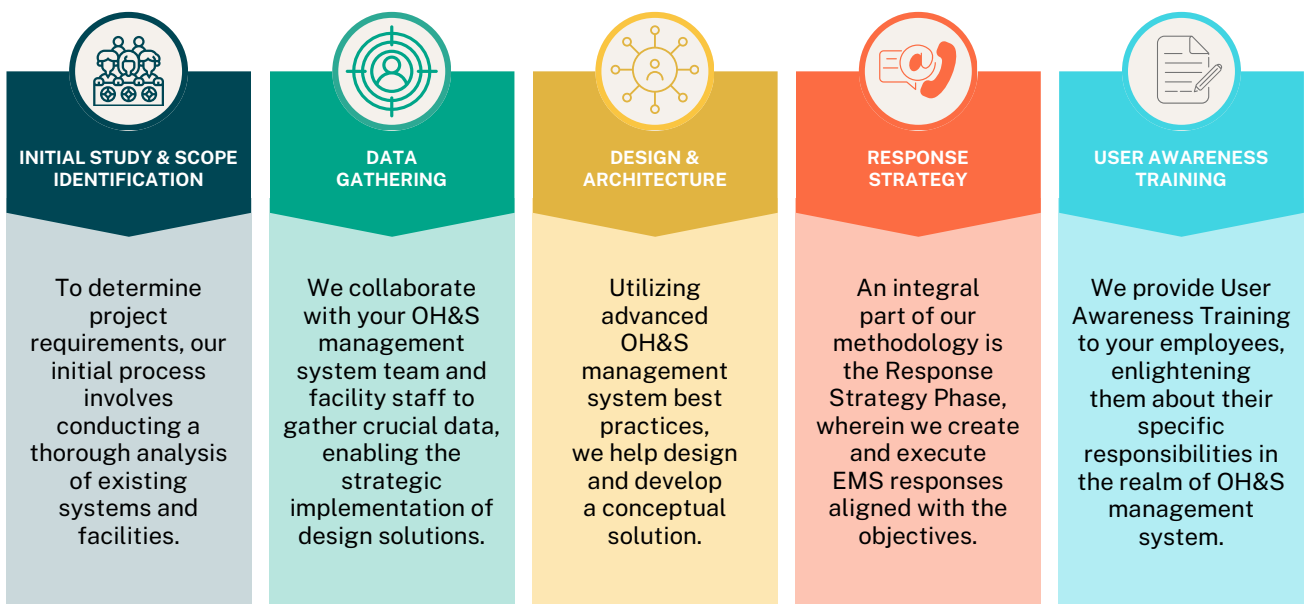
## ISO 45001 Benefits

ISO 45001 helps organizations identify and assess occupational health and safety risks, leading to improved safety performance. It can help organizations meet legal and regulatory requirements related to occupational health and safety.

A reduction in workplace accidents and incidents can lead to lower costs associated with medical treatment, compensation, and insurance premiums. ISO 45001 encourages effective communication about occupational health and safety issues within the organization. Increased awareness among employees can lead to better hazard reporting and a quicker response to emerging risks.



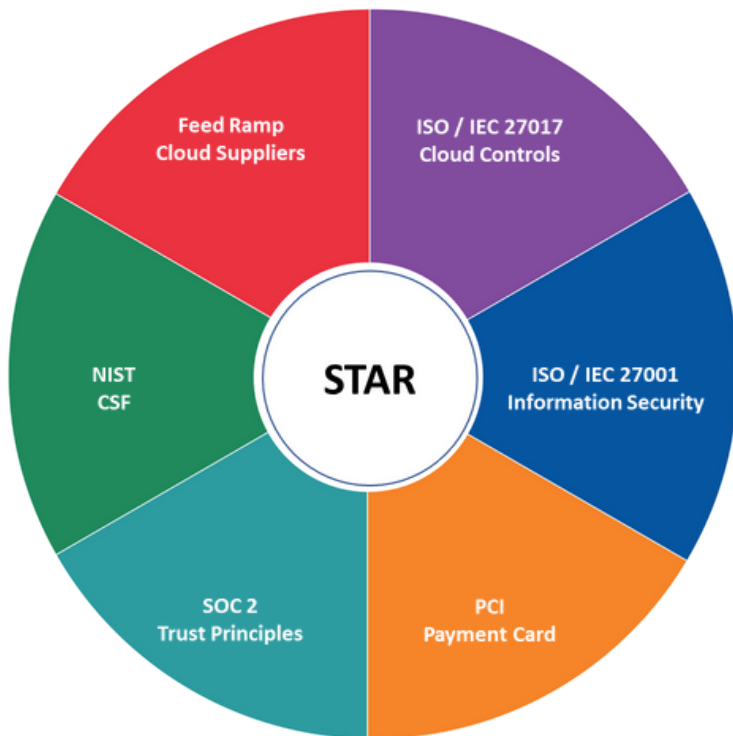
## Cyber Matterz approaches to ISO 45001



# CSA STAR

A CSA Security, Trust, Assurance, and Risk (STAR) certification is a powerful third-party attestation of a cloud service provider's security practices. A cloud service provider that earns a STAR certification can assure their customers that they're using industry-leading best practices to secure data in cloud applications.

## Using CSA STAR to integrate your security systems



## Levels of STAR

### CSA STAR Level 1

STAR Level 1 is designed for low-risk environments. The simplest option, it allows organizations to self-certify their compliance. Each CSP's documentation is made public on the CSA Register.

### CSA STAR Level 2

STAR Level 2 is recommended for medium-risk and medium-maturity environments, as well as organizations that wish to provide a higher level of assurance for their products or services.

### CSA STAR Level 3

STAR Level 3 is designed for high-risk environments and full-service providers. It provides the highest level of transparency into an organization's cloud security controls. Level 3 is based on the concept of continuous effort.

## STAR vs SOC 2

The CSA STAR Attestation is actually a combination of SOC 2 plus additional cloud security criteria from the CSA CCM. It provides guidelines for CPAs to conduct the SOC 2 engagements using criteria from both the AICPA and additional cloud-specific criteria from the CSA Cloud Controls Matrix.

## STAR vs ISO 27001

The CSA STAR Certification leverages the regular requirements of the ISO 27001 management system standard together with the cloud-specific requirements from the CSA Cloud Controls Matrix.

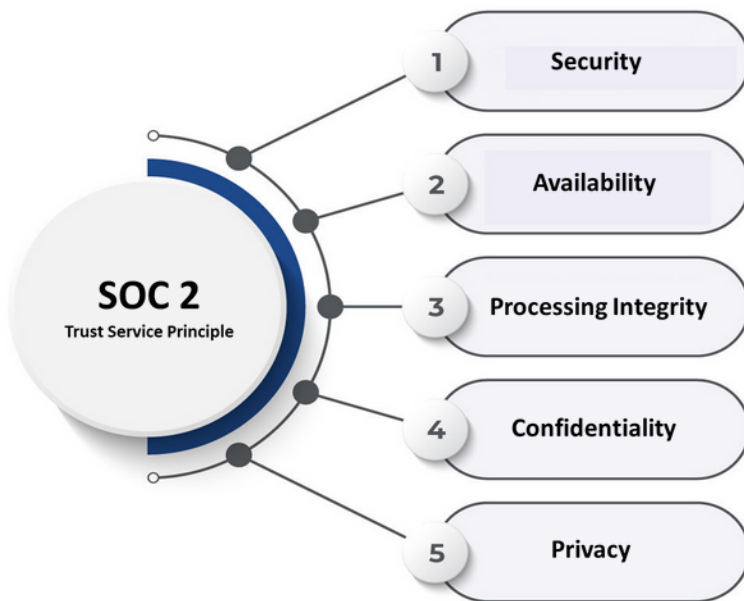




# SOC 2

SOC 2 compliance is part of the American Institute of CPAs' Service Organization Control reporting platform. It intends to ensure the safety and privacy of your customers' data. It outlines five trust service principles of security, availability, processing integrity, confidentiality, and privacy of customer data as a framework for safeguarding data.

## SOC 2 Principles



## How does ISO 9001 works?

### Security:

Protect systems from malicious attacks, data loss, and other security events.

### Availability:

Ensure that systems maintain high availability.

### Confidentiality:

Quality assurance processing monitoring.

### Confidentiality:

Ensure that confidential information is protected from unauthorized access.

### Privacy:

Ensure that personal information is protected from unauthorized access.

## The different SOC Reports

The SOC 2 standards focus on the non-financial reporting on the internal controls and systems that you can implement to protect the confidentiality and privacy of data that are stored in cloud environments. It Relevant for any service organization storing customer data in the cloud, managing sensitive information, or providing services like data hosting and processing.

SOC 1 report is a report generated by auditors for other auditors, but a SOC 2 report usually has more confidential internal information which is not to be shared with others outside the company. SOC 2 report provides details about the nature of those internal controls.

## SOC 2 compliance

It refers to an organization's adherence to the criteria set out in the SOC 2 framework. It is particularly relevant for technology and cloud computing organizations that handle sensitive information. It is based on five trust service criteria that serve as the foundation for evaluating and reporting on the controls in place.

