DTS

DTS
Information Security

Information Security

Information security is the prerequisite for successful digitalization. Different specifications, best practices, standards and certifications provide a solid technical foundation and a comprehensive tool for this. This comprises methods, instructions, recommendations and self-help assistance for authorities, companies and institutions that want to address the security of their data, systems and information. The key is to take a holistic approach to information security: In addition to technical aspects, infrastructural, organizational and personnel issues are considered. This allows a systematic approach to identifying and implementing the necessary safety measures. This is how the BSI defines information security.

The integrated approach mentioned above is our top priority in all areas, i.e. starting with the strategy and the corresponding guidelines, through the resulting processes, to workshops and IT security solutions. This ensures that everything interacts properly. Our experts are at your disposal with comprehensive advice and services. We work with you to create customized solutions and support you in every conceivable aspect of information security.

- Establishment, implementation & maintenance of an information security management system (ISMS)
- Preparation for certifications & requirements resulting from information security
  - Consulting for: ISO 27001/27002, ISO 27019 & IT-SiKat, TISAX®, BSI Baseline Protection based on ISO27001, KRITIS, EU-GDPR
- System audits/first audits/internal audits
- Emergency management
- Risk management/risk assessment
  - BSI 200-3, ISO27005
- Crisis communication/crisis management
- Individual training & awareness concepts

The advantages we offer

Pragmatic approach to solutions
We adapt your processes and security measures so that they can be integrated and put into practice in your company in a way that saves resources.

Lower costs
Our pragmatic approach saves on project costs and work.

Experience in the field of information security
Through a wide variety of projects in all kinds of industries, we bring interdisciplinary experience and expertise to the table.

Reports & recommendations for action
On request, you will receive detailed reports on all stages and processes, including recommendations for action adapted to your company structure.

Information Security Management System (ISMS)

It is not only since digitalization that information has been one of the most valuable assets of a company, and one that requires extensive protection. Business secrets, production processes, customer information – protection from misuse, loss or theft is essential. In this context, information security refers to both digital and analog data. A sustainable strategy ensures that the protection goals of information security are achieved or maintained.

- Integrity of systems, data and necessary changes
- Data confidentiality
- Availability of systems and data
- Authenticity of information and sources
- Commitment for processes, actions, system components
- Resilience of IT systems

The Service

Achieving a level of security for all of an organization's business processes, information, and IT systems that meets its needs requires more than just purchasing anti-virus protection and firewalls or backing up data. An integrated approach is important. Above all, this includes a functioning safety management system that is integrated into the organization. Information security management is the part of general risk management that is designed to ensure the confidentiality, integrity and availability of information, business processes, applications and IT systems. This is a continuous process, the strategies and concepts of which must be constantly reviewed in terms of performance and effectiveness and updated as necessary. Information security is not just a question of technology, but depends to a considerable extent on the organizational and personnel framework.

More and more business processes are being linked via information and communications technology. This goes hand in hand with the increasing complexity of technical systems and a high reliance on correctly functioning technology. A planned and organized approach by all stakeholders is therefore necessary to enforce and maintain an appropriate and adequate level of security. Integration of this process into all business units can only be ensured if it becomes the responsibility of the top management level. Top management is responsible for proper and effective functioning of an organization and thus also for ensuring information security both internally and externally. It must therefore initiate, control and monitor the security process. This includes strategic guidance on information security, conceptual specifications and organizational framework conditions and adequate resources to achieve information security in all business processes.

(Source: BSI Bund 200-2 Baseline Protection Standard)

What does DTS offer?

A security strategy is required across all areas of a company or an authority to ensure that its most important business processes run smoothly in the long term. The integration of an ISMS can prove to be quite complex in practice. It is essential that the security concept is integrated into existing organizational structures and operational processes and that the business processes of an organization are not fundamentally changed. The following challenges must be considered:

- Structure and definition of the areas covered by an ISMS
- Determination of the scope
- Establishment of the necessary security organization and security process
- Development of an appropriate security strategy and security objectives
- Integration of the information security strategy into the existing corporate strategy
- Selection of suitable security measures

- Maintenance and continuous improvement of the safety level achieved
- Clear demarcation between data protection and IT security
- Establishment of suitable security organization

We support you throughout the design and implementation of your ISMS according to ISO 27001 or similar standards. The PDCA cycle is used as the basis for implementing an ISMS. The introduction of an ISMS is divided into the planning phase, implementation phase, review and revision phase, and improvement phase with corresponding redesign. The project is managed throughout by Mr. Sven Meier, a trained and certified IT security officer (ISO, BSI Baseline Protection, TISAX, etc.) since 2012. He is responsible for the project and the resources used. During the project phase, appropriate performance indicators are defined that can measure and evaluate the effectiveness of an ISMS.

Preparation for information security certifications

We prepare you for all important certifications of information security, advise you on all necessary aspects and jointly develop concepts and strategies.

- ISO 27001 & 27002 consulting
- ISO 27019 & IT-SiKat consulting
- TISAX® consulting
- BSI Baseline Protection
- KRITIS consulting
- EU-GDPR consulting / ISO 27018

The Service

ISO 27001 & 27002 consulting

Various laws require information technology to be considered in an attributable and integrated way and legally binding proof of protective measures to be provided. In addition, information security is an ever-increasing success and trust factor for companies and institutions. The international standard ISO/IEC 27001 represents one of the best known and most widely recognized frameworks in the international environment for representing a reliable information security management system.

Any implementation of ISO/IEC 27001 stands or falls with a scoping process aligned with an organization's business strategy. The challenge is to find the ideal balance between economic and functional aspects. In the context of a GAP analysis, we define the measures necessary to meet the requirements.

We determine at an early stage of the project which measures must be implemented directly and areas where later implementation will suffice. Our results show you concrete potential for improvement. On the basis of a reliable project plan, which shows all the work and time specifications, you can decide for yourself where we are able to support you.

(Source: www.hisolutions.com/security-consulting/informationssicherheit/iso-27001)

ISO 27019 & IT-SiKat Consulting – Standard for information security in the energy utility industry

The international standard on information security for the energy utility industry sets out the guideline for an information security management system (ISMS) that pursues the goal of ensuring functional and reliable operation of control and automation technology. This involves systems and networks for controlling, regulating and monitoring the extraction, generation, transmission, storage and distribution of electrical energy, gas, oil and heat. The term process control technology includes communication technology as well as control, automation, protection, safety and measurement systems. A holistic view that includes the associated IT and OT systems is essential to ensure a reliable power supply. All processes and systems applied within an organization must also be considered. The updated standard requires, for example, that operators of critical infrastructure in the energy sector demand an equivalent level of security from relevant service providers and document this. The process is analogous to certification according to ISO 27001.

Benefits of ISO 27001 or 27019 certification:

- Internationally accredited proof of the effectiveness of the security concept
- Stronger legal certainty in critical security matters
- Systematic realization of the protection goals of information security
- Maintenance and continuous increase of the security level
- Integration of appropriate measures to provide protection against all types of threats
- Strengthening of the security awareness of employees
- Building trust with regard to cooperation with external organizations

TISAX® Consulting
Procedure for TISAX certification:

- Definition of the scope and assessment level
- Kick-off, document review and self-assessment
- On-site assessment or remote assessment with interim report
- Planning, approval, implementation and subsequent evaluation of corrective actions
- Effectiveness audit
- Posting of the final report to the TISAX® online platform and issuing of the test labels

Advantages for a company:

- Gaining the trust of all stakeholders
- Meeting the needs and requirements of suppliers and customers
- Fulfilling the high safety requirements of the automotive industry
- International recognition of the safety level by the automotive industry
- Avoiding multiple certifications and assessments
- Time and cost savings through greater efficiency
- Greater transparency along the entire supply chain
- Anchoring information security in the company
- Continuous maintenance of the information security level once achieved
- Competitive advantage through differentiation from market competitors

BSI Baseline Protection based on ISO27001 Consulting
The IT Baseline Protection methodology is defined in BSI Standard 200-2 and contains a practical description of how to set up and operate an ISMS. The main topics here are:

- Role of the ISMS
- Establishment of organizational structure of the IS
- Selection of the security requirements & implementation of the security concept
- Continuous improvement and maintenance of the IS
- Selecting the approach or level of protection based on the initial assessment so that IT Baseline Protection can be adapted to the requirements of organizations of different sizes, industries and functions according to protection requirements.
- Target: Cost-effective and targeted ISMS, reduction in work
    - Basic
        - Entry point into the security process
        - Initiation of an ISMS

        - Reduction of risks as quickly as possible
        - Subsequent detailed analysis of the actual safety requirements
    - Standard
        - Comprehensive and in-depth methodology
        - BSI preferred approach
        - ISO 27001 compatible
    - Core
        - In-depth protection of particularly important business processes and assets
        - Also possible as an entry point into the security process to secure particularly vulnerable business areas

KRITIS consulting

The German Federal IT Security Act passed in 2021 consolidates the role of the BSI (Federal Office for Information Security) as the central authority for information security and digitalization. As Germany's cyber security authority, it has far-reaching powers and authority to identify security vulnerabilities or prohibit the use of critical components in security-critical areas. A central component of the revised law is the change with regard to the security of critical infrastructure operators and their systems. CRITIS (critical infrastructure) regulation has been significantly expanded by the IT Security Act 2.0. The following changes have come into force in the course of this:

- Detection of attacks must be implemented on a mandatory basis for operators of critical infrastructures. In practice, this requirement can be addressed by a SIEM and a SOC.
- In the event of a malfunction, CRITIS operators and UNBÖFI are obliged to provide the BSI with all data required to manage the disruption on request.
- The Ministry of the Interior must be notified of the use of critical components by CRITIS operators in certain sectors. Critical components are IT products in CRITIS facilities on whose functionality the operation of the facility significantly depends and in which a failure of such a component would have a significant impact on the function of the facility.
- Immediately after being identified as a CRITIS operator, they must register with the BSI and designate a contact point.
- The scope of the CRITIS sectors was extended to include the municipal waste management sector and thresholds for critical infrastructure operators were significantly lowered, while new CRITIS facilities were added.

Our custom-fit ISMS CRITIS concept is delivered with you and for you in the following phases:

- Phase 1: Workshop/coaching to define the basic structures
- Phase 2: Establishment and integration of an information security management system
- Phase 3: Implementation of the defined information security measures at the sites
- Phase 4: Support for the audit according to Section 8a CRITIS Regulation

EU-GDPR Consulting / ISO 27018 as an internationally certified cloud standard

This standard sets out data protection requirements that deal with processing of personal data for cloud service providers. ISO 27018 certification is a decisive criterion for many when selecting a cloud service provider. Accordingly, the advantages of this certification are:

- Competitive advantage through differentiation from market competitors
- Strengthening the confidence of potential customers in your company
- High level of compliance with the GDPR and the EU Data Protection Directive

System audits / First audits / Internal audits

How far has your company progressed in the information security certification process? Whether ISO 27001, BSI Baseline Protection, TISAX® or other information security requirements – we conduct system audits based on your defined requirements to verify the compliance of your entire information security management system or parts of it. In doing so, we look at and evaluate the documentation, but also make appropriate on-site assessments of the premises.

- System audits
- First audits
- Internal audits
- ISO 27001, BSI Basic Protection, TISAX® etc.

The Service

The process consists of the following phases:

Phase 1:

- Preparatory kickoff
- Identification of the contacts required
- Coordination of interview dates
- Review of customer documentation to gain an understanding of the regulations

Phase 2:

- Implementation of the system audit on site on the customer's premises
- Auditing of actual practice in processes
- Auditing of the specification and verification documentation
- Auditing of the physical and spatial conditions on the customer's premises including buildings and infrastructure
- Identification of GAPs (loopholes in measures)

Phase 3:

- Preparation of a detailed audit report with recommendations for action (reference action targets)
- Discussion and presentation of the results to the management on request

Phase 4:

- Preparation of an action plan based on the findings
- Development of a project plan for the implementation of the reference actions that have not been completed.
- Support in carrying out the actions through to successful completion
- Effectiveness testing

Emergency management

Our concept includes methods and measures for the integration of emergency management in the organizations and institutions of Mediengruppe Oberfranken. The services offered are based on the current Standard 200-4 of the BSI. However, the individual activities can also be defined according to other standards.

- Integrated emergency management concept
- Requirements assessment, preliminary analysis and target/actual comparison
- Guidelines with definition of all main processes
- Establishment of concrete emergency plans
- Review, evaluation & optimization of emergency plans

The Service

Services offered include:

- Phase 1: Initialization, preliminary analysis & BIA - Kickoff concept workshop
    - Requirements assessment of the motivation of the BCM
    - Requirements assessment of the BCM period to be covered
    - Requirements assessment for determination of criticalities/MTPD/RTO/RPO
    - Requirement assessment of existing resources
    - Requirements assessment of systems
    - Requirements assessment of critical systems in use
    - Requirements assessment of the communication architecture
    - Options for structuring and setting up reactive emergency documentation
    - Adoption of the results from risk management and hazard definitions
    - Determination of the substantive objectives and scope of application
    - Review of current sources of information and documentation
    - Distinction from/extension to include operating manuals and guidelines
    - Assessment of the internal and external organizational structure
    - Preliminary analysis for the BIA
    - Business Impact Analysis
    - Target/actual comparison
    - GFP

- Phase 2: Creation of BCM plans for main processes - Creation of a document template for defining guidelines.
    - Motivation for the development of the BCM
    - Definition of the period to be covered
    - Scope of the BCM
    - Definition of overall responsibility

- Definition of responsibilities in the BCM
- Definition of the BCM and the escalation levels “fault”, “emergency”, “crisis”
- Definition of network communication
- Definition of cryptography
- Central roles in the BCMS
- Available resources

- Phase 3: Creation of IT emergency plans - Guidelines for the creation of a special organizational structure (BAO)
  - Set-up of an emergency/crisis team
  - Set-up of the core team
  - Set-up of the situational extension (optional)
  - Set-up of the staff assistance
  - Set-up of the emergency response team
  - Definition/creation of the reporting path
  - Specifications of the methods and rules for staff work
  - Specifications for communication during an emergency response
  - Definition of the criteria for de-escalation
  - Definition of the criteria for dissolution of the special organizational structure
  - Analysis of the response
  - Creation or expansion of emergency plans
  - Maintenance and control of emergency management

- Phase 4: Test & practice - The measures defined and implemented are tested with those responsible at Mediengruppe Oberfranken after successful integration.
  - Review of the BCM

- Phase 5: Optimization
  - Support in the optimization process

Risk management / Risk assessment

We provide you with a fully comprehensive risk management and/or risk assessment according to BSI Standard 200-3 and ISO 27005.

- BSI Standard 200-3
- ISO 27005
- Risk analysis, assessment, treatment & monitoring

The Service

BSI Standard 200-3

The risk analysis process is a recognized and proven way to achieve a predefined level of information security with minimum effort. Based on elementary hazards, which are set out in the IT Baseline Protection Compendium, a risk assessment for areas with a normal need for protection is already included in the development of the IT Baseline Protection modules. The advantage of this method is that users of IT Baseline Protection do not need to conduct a separate threat and vulnerability analysis for most information systems, as this has been carried out in advance by the BSI.

However, if the information network under consideration contains target objects that have a high protection requirement, that cannot be fully modeled with the existing building blocks of IT Baseline Protection or that are operated in environments that are not covered by IT Baseline Protection, a risk analysis is mandatory.

ISO 27005

- Definition of the framework conditions
  - Definition of the area under consideration
  - Establishment of organization for risk management
  - Definition of method
  - Establishment of criteria for evaluation, acceptance and impact
- Identification of risks
  - Recording of all company assets. This includes information, business processes, personnel, organizations and IT components
  - Identification of all relevant threats and existing vulnerabilities
  - Identification of existing and planned security measures
  - Identification of potential consequences that could arise if relevant threats materialize
- Risk analysis
  - Assessment of the extent of damage in the event of a breach of one of the information security protection objectives (confidentiality, integrity or availability)
  - Determination of the probability of occurrence of a threat
  - A combination of the extent of damage and the probability of occurrence can be used to determine the risk level
- Risk assessment
  - The prioritization of risks based on the risk level and the evaluation and acceptance criteria forms the decision-making basis for subsequent risk treatment
- Treatment of risks
  - By creating a risk treatment plan based on the overall picture of risks, it is possible to decide how to treat the identified risks. On the basis of the economic consequences of the risks relative to the implementation costs of

appropriate precautions, decisions are then made about how to address the risks. Typically, risk treatment options fall into one of the following four categories

    - Decision as to whether a risk
        - is reduced with the aid of appropriate security measures
        - remains untreated, given that it meets the acceptance criteria for residual risks
        - is prevented by avoiding certain processes or activities
        - is shared with a third party (e.g. insurance company) by means of an appropriate transfer

- Acceptance of risks
    - Based on the risk treatment plan, the management of an organization decides on the recommendations for action it contains for the purpose of implementing the measures, taking into account the use of resources. Risks for which no action is taken must be accepted.
- Communication of risks
    - In order to ensure that the results and methods applied are up-to-date, constant communication of information about risks is required between risk management and decision-makers. It is advisable to involve other relevant employees as necessary and to share information with them at all times.
- Monitoring and reviewing risks
    - All influences on risk management must be monitored for changes at all times. As the business and technological environment is always undergoing a process of change, these changes have an impact on the threats to an organization and its vulnerabilities. The approach to risk management should also be reviewed for appropriateness at regular intervals.

Crisis communication

We are unique in the IT sector in offering you an integrated concept for crisis communication, from concept kick-off through to defining and updating crisis management structures.

- Crisis communication concept, including kick-off
- Preparation of crisis communication
- Definition & adaptation of communication structures
- Development of a crisis communication plan
- Update of the crisis management structures

The Service

- Concept kick-off
    - Requirements assessment of the corporate structures, the established emergency and crisis management, the communication architecture
    - Review of documentation sources
- (1) Preparing crisis communication
    - Definition of the basic and organizational framework for crisis communication
    - Development/implementation/testing of the crisis communication cycle
    - Evaluation/testing/updating of communication/information flows
- (2) Defining/updating communication structures within the crisis team
    - Definition/evaluation of target-group-oriented communication
    - Determination of communication structures within/outside the organization
    - Definition of the press tasks
- (3) Developing a crisis communication plan
    - Preparatory measures for the communication plan & development of an action plan
- (4) Defining and updating crisis management structures
    - Definition of the responsibilities, competencies and roles of the crisis team
    - Definition of the communication channels
    - Checking of the situation center and equipment
    - Public relations guidelines
    - Documentation template for logging

Individual training & awareness concepts

Awareness campaigns and an e-learning platform are not always sufficient to meet the needs of users/employees and provide them with access. We offer individual training concepts that are tailored to your requirements, we create them according to your needs and implement them in your training system in the form of a training video or a face-to-face event.

- Training and awareness concepts
- Customized
- Implementation in existing training systems
- Training videos
- Training on site

DTS Systeme GmbH
+49 5221 1013-000

DTS Systeme Münster GmbH
+49 251 6060-0

dts.de
info@dts.de