Intervalid ISMS

Information security management system

Comply easily with policies and standards

Is your company safe?

Technological progress is changing the way we do business. And while this offers many opportunities, it also presents information security risks caused by technical or human errors or actions, such as hacker attacks, data breaches and many more. Companies have no choice but to address such vulnerabilities if they want to avoid high fines, remediation costs, or reputational damage. Guidelines such as ISO 27001, BSI IT-Grundschutz, VdS 10000, TISAX®*, ISIS12/CISIS12 or the B3S make a significant contribution to the security of company-wide information.

How do you implement these extensive guidelines?

An information security management system (ISMS) comprises standardized procedures and policies, and specified measures, to protect corporate assets and minimize risks. Regardless of whether you have your company certified, the requirements according to the standard you have chosen (e.g.: ISO 27001) must be met. This is the only way to identify security risks in advance and take appropriate measures. The use of a structured ISMS offers you efficient support and also saves time, human resources and costs.

The reasons for an ISMS implementation with software

Significant time savings

Employees spend a significant amount of time gathering information and documenting. Use structured sample templates, checklists and workflows to speed up this process and refocus on core tasks.

Improved quality

Uniform templates provide a structured preparation. These create a low error rate and clear documentation. Regular updates ensure that the company can monitor compliance in real time. Hence, the use of software allows companies to easily and quickly achieve the desired quality standards in their information security processes.

Increased security

Intervalid ISMS can identify gaps, provide checklists and workflows for remediation and conduct regular audits. All entries and changes are logged and can be traced at any time. In this way, your company can benefit from continued confidence in its information security.

All-in-one solution

Intervalid ISMS offers a central solution that covers all requirements in one system. One of the most valuable aspects is the collaboration between colleagues from various departments: The digital involvement of employees and their active participation accelerates implementation and helps to keep information up to date.

Advanced functionality

In addition to the technological aspects, the software offers the user dedicated functions to solve certain problems. Such additional functions, such as automated translation, offer users practical solutions.

Increase productivity - reduce costs

With Intervalid ISMS you receive a comprehensive solution to information security requirements - without having to start from scratch. ++++No special knowhow is required and the training outlay is very low. This saves you additional costs and ensures that you are safely prepared for audits.

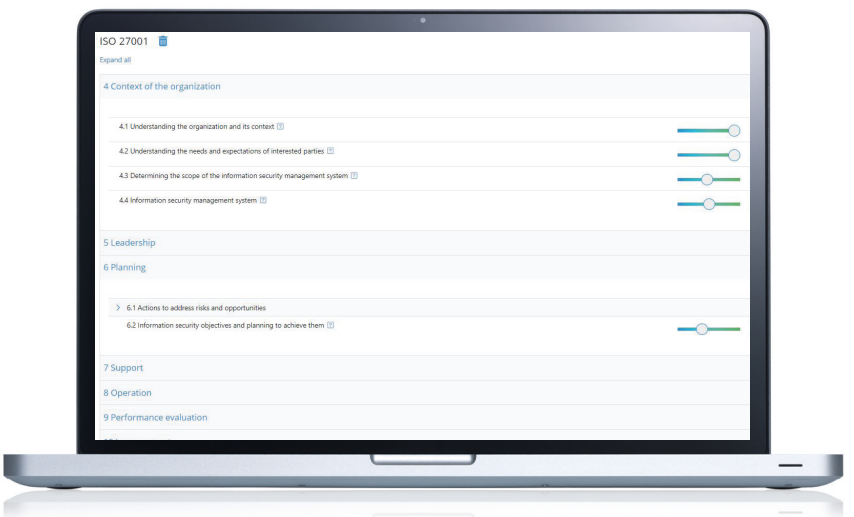
Comprehensive information security management
How Intervalid ISMS supports your business

The team of Intervalid works on the up-to-dateness and functionality of the software. With the structured tool, you are guided step-by-step through the standardized templates such as ISO 27001, BSI IT-Grundschutz, VdS 10000, TISAX®, ISIS12/CISIS12 or B3S and actively involve your employees. The software offers you all the mandatory documents for certification according to ISO 27001. This shortens the implementation time enormously and continuously increases the information security in your company. The tool includes contingency planning and ensures your business continuity management (BCM).

Intervalid ISMS
Product features in detail

Intervalid was developed as Software as a Service (SaaS) and is installed in an ISO 27001-certified data center. All you need for implementation is an internet connection and you can start immediately. The solution is also available as an on-premises version.

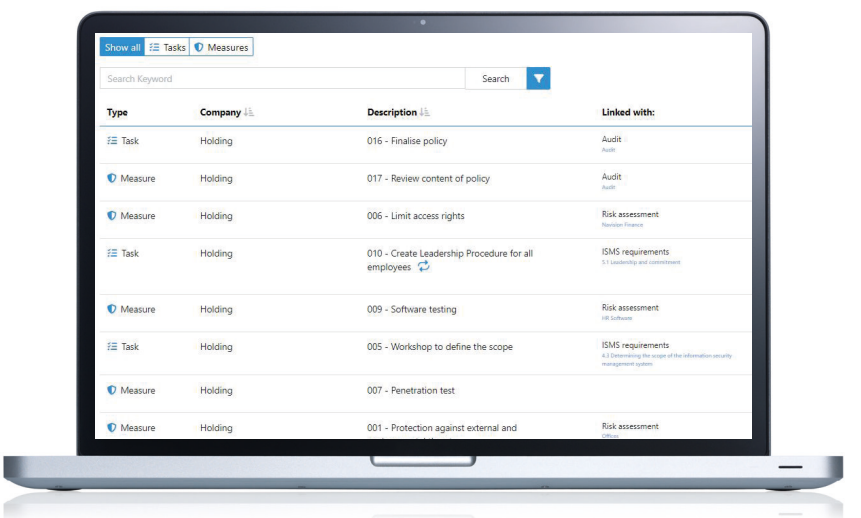
ISMS policies
Meet all your ISMS requirements



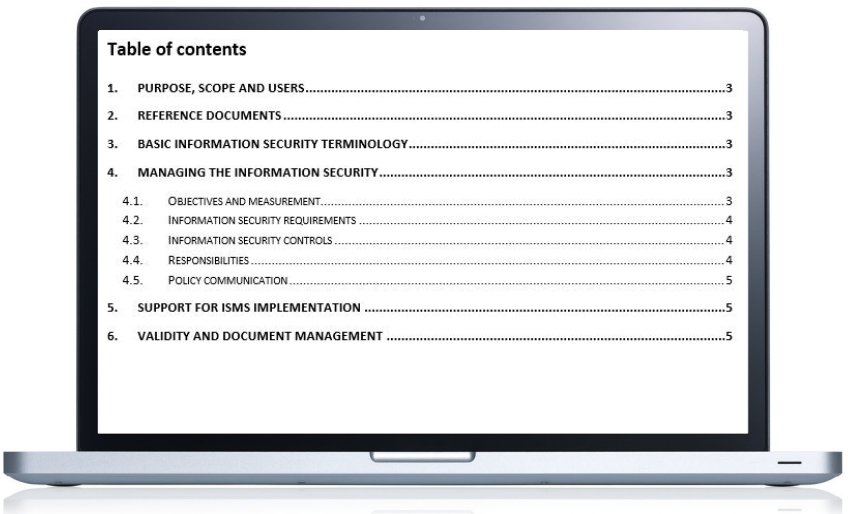
When establishing an ISMS for your company, the first decision is which standards or policies you want to follow. There are standardized templates for ISO 27001, BSI IT-Grundschutz, VdS 10000, TISAX®, ISIS12/CISIS12, and B3S. All requirements, responsible employees, current progress, as well as associated tasks are clearly displayed on one screen. This function allows you to control the entire ISMS process across your company.

Tasks and measures workflow
Create, distribute and edit tasks

When implementing an ISMS, the cooperation of all departments is crucial for success: Set tasks, including deadlines and distribute them to the responsible employees. Each user has their own task list and the current project status is visible at all times. This means all employees are actively involved in the process.



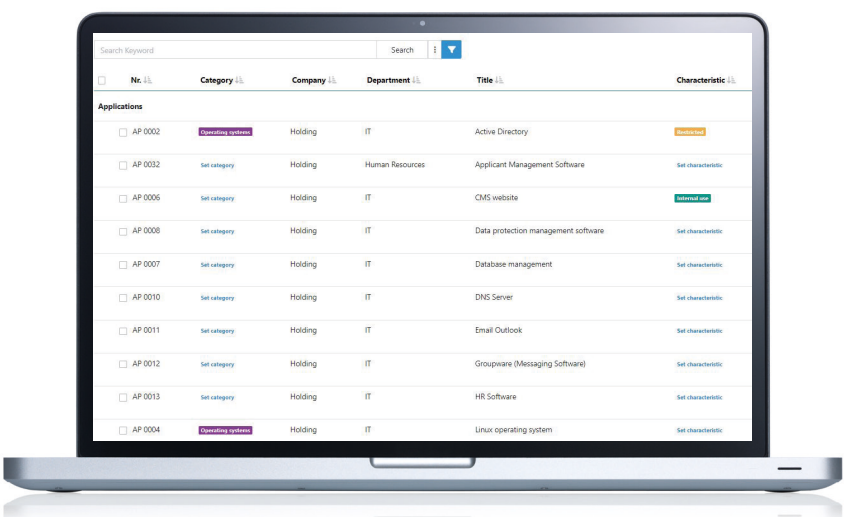
Internal policies and processes
Draw up and maintain company-wide rules



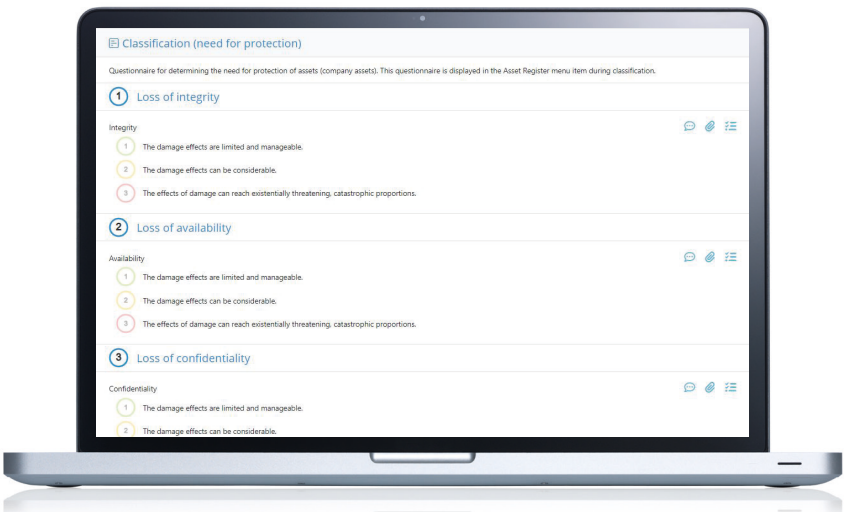
To minimize security risks within your company, employees must be made aware of both the risks and the appropriate procedures they are required to follow. To achieve this, sample templates are available to create the necessary policies and processes for your organization. These form the foundation for ISMS implementation, as they will be followed by all employees. The documents should be regularly maintained and kept up to date, to ensure consistent and structured implementation throughout your organization.

Asset register
Display your assets in a structured form

This function allows you to capture and group your assets in a structured register. To make this process as efficient as possible, you can either use a template or import the data. You will need to define a responsible person (owner) for each asset. The workflow can then be used to log new assets or to report changes to existing ones. The technical and organizational measures (TOMs) can be set out either via a template or in a personalized form for your company. The register is clear, multilingual, easy to use and offers customizable selection options.



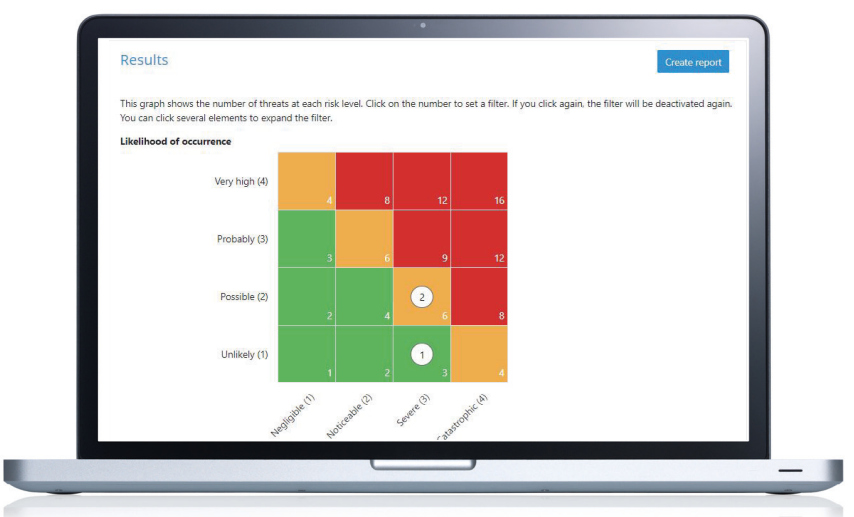
Assets classification
Evaluate the level of protection for your assets



This is where the level of protection for each of your assets is determined. Business-critical assets, particularly those of high importance to your company in terms of information security, are identified. The responsible employee assesses the protection level required for each asset with the help of predefined risk levels. This lays the foundation for risk analysis.

Risk analysis
Recognizing risks

This step initiates a risk analysis for all assets that require a high level of protection. You will receive a number of sample templates and questionnaires for this purpose, and will be guided systematically through the process in order to identify the potential hazards. Next, you can determine the risk and obtain recommended measures to address such risk. After prioritization and cost estimation, the result can be forwarded to the management for approval.

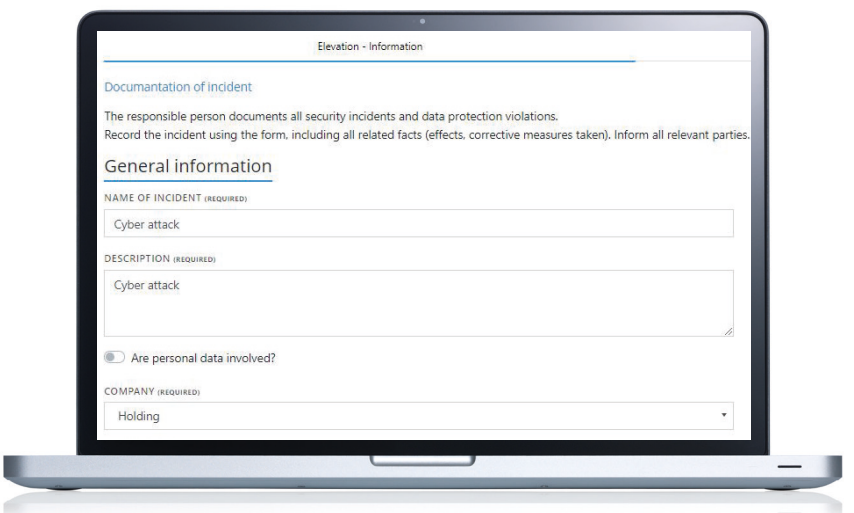


Contingency planning (BCM)
Prepare for an emergency

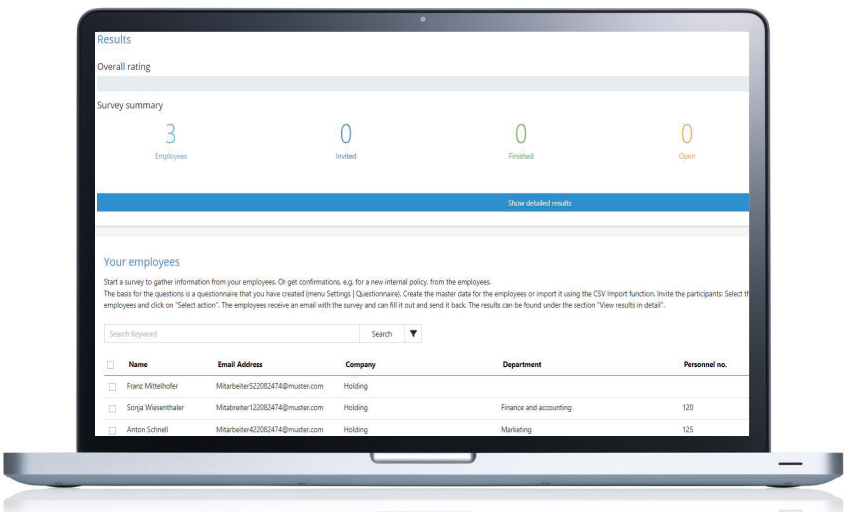
Conduct a business impact analysis to identify those business processes that are business critical for your organisation. You will be guided through the process with assistance. As a result, you will see the maximum tolerable downtime and recovery time for your assets. In the next step, create the recovery plan for the critical processes. The final emergency plan is created at the push of a button.

Security incidents workflow
Respond properly to security incidents

Use this function to respond to security incidents correctly and quickly: Record the key data, analyze the incident, inform all relevant departments in a timely manner and take preventive measures.



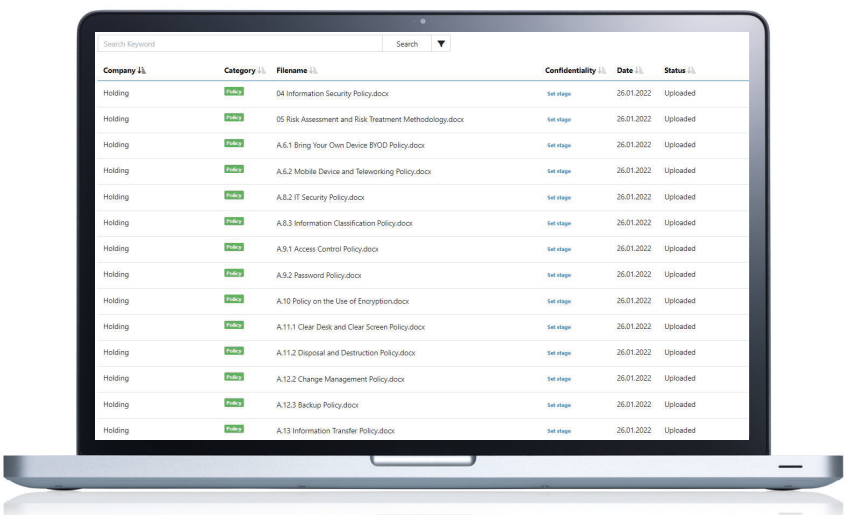
Surveys and monitoring
Ascertain level of knowledge of those within your organization



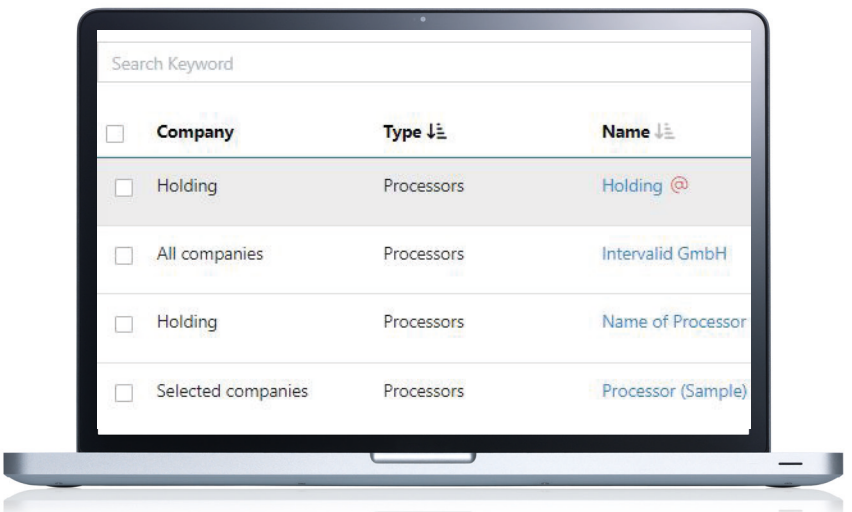
Obtain information about the current knowledge levels of your employees via a template survey or a customized one. Once the survey has been completed, Intervalid produces a clear summary of the results, allowing you to see where there might be gaps in the employees' knowledge. This function can also be used to easily confirm that the employees have read and acknowledged the relevant policies.

Document templates
Easily created online

Create templates for your corporate documents such as information security reports, policies, contracts and more. Numerous formatting options are available for this purpose and you can also use variables to automatically insert content into the document. The documents can then be forwarded to the responsible user for editing or approval. In this way, you are able to manage your company documents centrally, are always aware of their status and can make them available to your employees.



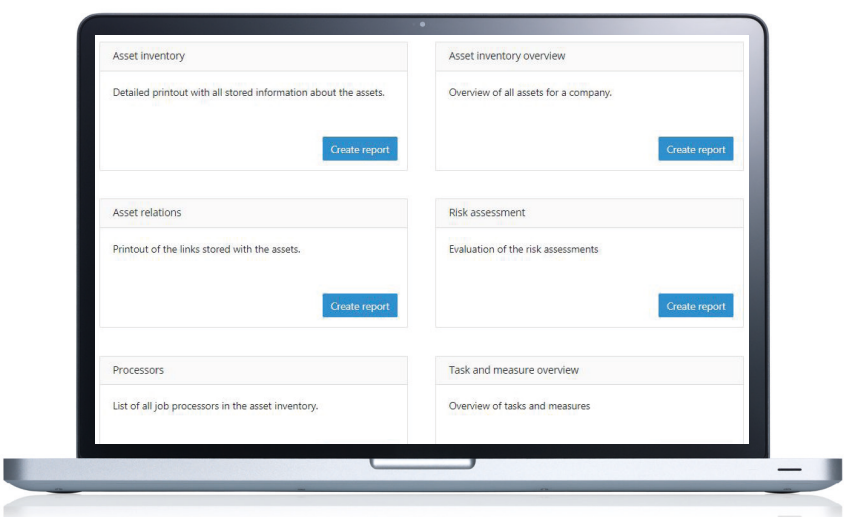
Supplier audit
Check your processors and suppliers



Supplier audits are used to check new or existing suppliers and processors in terms of information security compliance. The details of the contact person at the business partner will be entered and stored in the system. Then you can send them a questionnaire or fill it out internally. After the form has been completed/ returned, you can distribute tasks as required and complete the audit. Finally, a date can be set for the next audit.

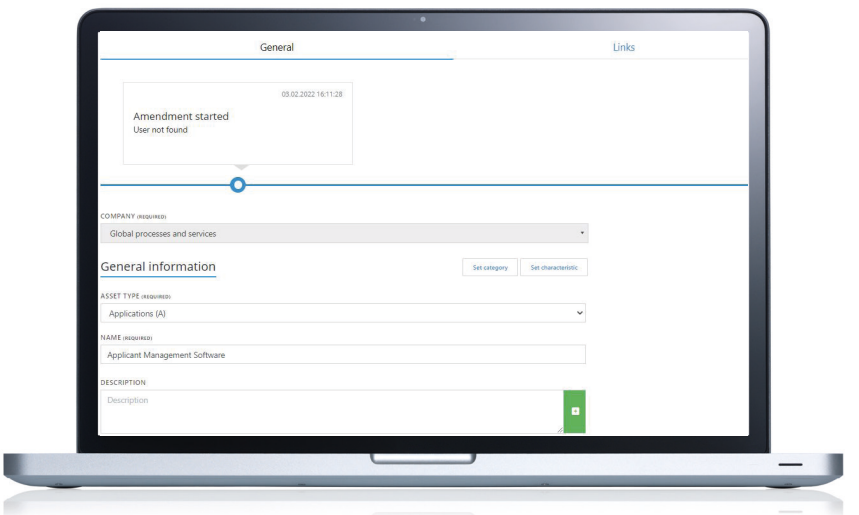
Reports and dashboard
Extract information quickly and obtain an overview

Create daily updated reports for internal or external purposes (e.g. audits, management reports, SoA, etc.) in the simple click of a button. The data can be exported via a CSV or a PDF file. This function allows you to monitor the current information security status of your company at any time, with all security incidents being documented transparently. The dashboard is configurable according to your requirements and provides a broad overview of the most important key data.



Audits and certification
Review your measures on an ongoing basis

The establishment of an ISMS does not come to an end once the requisite measures have been implemented. It is a continuous process according to the Plan-Do-Check-Act method and therefore the effectiveness of the ISMS must be assessed regularly. Use the system's monitoring features to carry out an internal audit or to prepare for certification. Run through your business processes regularly, optimize if necessary, identify new risks and thus continuously minimize your business risk.



Intervalid ISMS
For every company size and industry

The software was developed for **SMEs and corporations** that want to implant an **ISMS** according to the guidelines **ISO 27001, BSI IT-Grundschutz, VdS 10000, TISAX®, ISIS12/CISIS12, B3S**, etc. Larger companies with a number of international branches can benefit particularly from unlimited users, multilingual features (incl. automated translation) and clear group structures.

Your advantages with Intervalid ISMS

- ☑ Simple compliance with the guideline (such as ISO 27001, BSI IT-Grundschutz, TISAX®, B3S, etc.)
- ☑ Minimize errors through structured processing
- ☑ All requirements are covered within one system
- ☑ Easy implementation (SaaS development; also possible as on-premises installation)
- ☑ User-friendly interface
- ☑ Unlimited user & role definition (actively involve employees)
- ☑ Depict corporate structures

- ☑ Reduce effort through templates and intelligent functions (e.g.: automated translations)
- ☑ Current & transparent information in the klick of a button
- ☑ Ideal preparation for certification
- ☑ Updates provide the current status of the guidelines
- ☑ Incl. all mandatory documents and sample templates for all functions
- ☑ Integration of both modules (Intervalid ISMS & DSMS) in one system possible
- ☑ Save time and increase productivity

Excerpt from our reference list:

BONUS Vorsorge · BONUS Pension · HELL · HOERBIGER because performance counts · Nemak · STRECK TRANSPORT · AOF A&O FISCHER · abat · Fairmas · paperdoo DRUCKEN OHNE DRUCKER · HP · PRINZ · ACM-CONSULTANTS INFORMATIONSSICHERHEIT – DATENSCHUTZ · MAGENWIRTH TECHNOLOGIES

Get in touch to experience the benefits of Intervalid ISMS.

- Online demo
- Free trial
- Your individual offer

We will be glad to advise you.

intervalid

info@intervalid.com www.intervalid.com
AT: +43 1 905 10 44 GER: +49 721 1608 1337

Intervalid GmbH
Your contact in Austria

Am Heumarkt 11/1/2|1030 Vienna
T +43 1 905 10 44
M info@intervalid.at
W www.intervalid.com

Your contact in Germany

Unterreut 6 | 76135 Karlsruhe
T +49 721 160 813 37
M info@intervalid.de
W www.intervalid.com