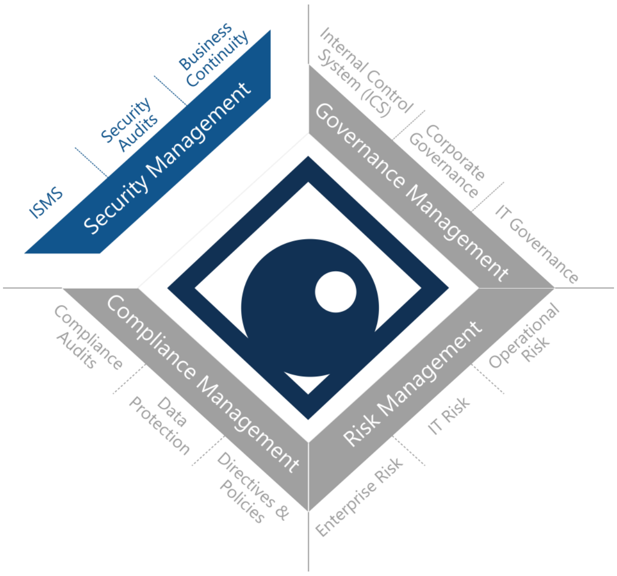
White paper

Information Security Management System (ISMS) using ibi systems iris



One purpose of ibi systems iris in security management is to support an ISMS

ibi systems iris provides a systematic and structured support for the initial setup and the further development of your information security management system (ISMS). Benefit from a group-wide approach according to best practice standards such as ISO/IEC 27001 or the NIST Cybersecurity Framework.

With ibi systems iris, you run your information security management system across the entire organization and describe its whole organizational structure, assets, processes as well as internal and external regulations. Thus, established standards such as ISO/IEC 27001 or the NIST Cybersecurity Framework can be applied and internal documents can be referenced.

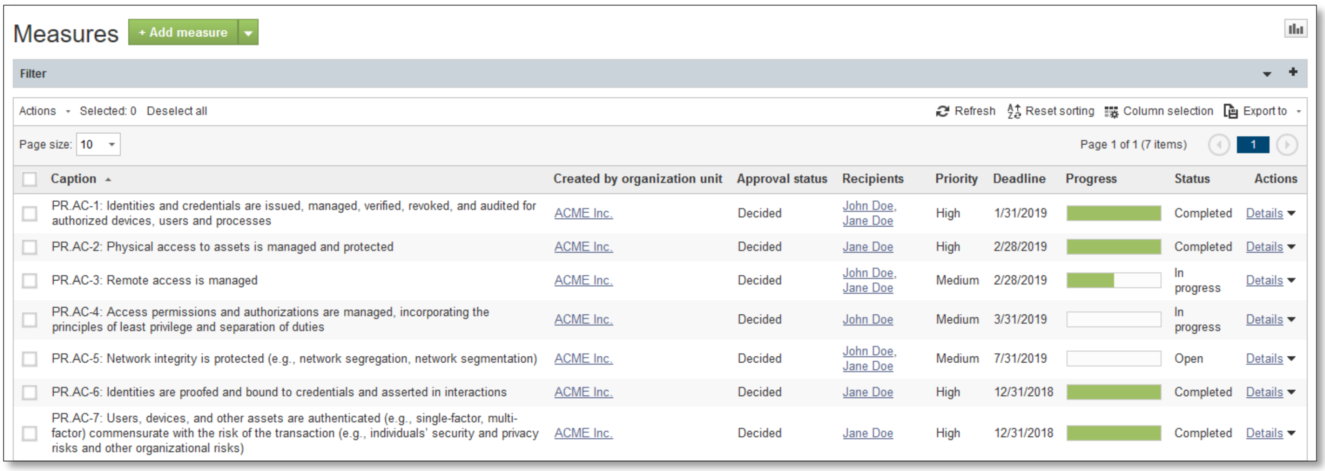
The NIST Cybersecurity Framework's flexible approach as well as all of ist functions (identify, protect, detect, respond and recover) are fully operationalized by ibi systems iris. As a first step, the business processes are identified and modeled to the relevant assets in scope. Protection requirements for availability, confidentiality and integrity can be assigned and inherited. Responsible organization units are assigned to both assets and processes. In order to categorize the processes and assets, you can use your own, even hierarchical, categories. These enable you to immediately derive risks and measures.

With ibi systems iris, you have full control of your ISMS at all times and an overview of critical risks, open measures and information security incidents.

> "ibi systems iris leads to significant cost savings and guarantees a business-oriented approach to solve increasing cybersecurity requirements.
>
> The special added value is the integrative applicability and the integrated know-how of best practice standards, controls or measures."
>
> *Dr. Stefan Wagner,*
> *ibi systems GmbH*

In assessments, findings such as vulnerabilities or improvements are identified. In turn, findings can create risks that need to be considered in regard of information security. In the subsequent risk analysis, the risk is assessed in the dimensions damage impact and likelihood of damage. The risk assessment is visualized in a risk map. After assessing the risk, the risk treatment option including its accompanying measures is defined. The implementation status of a measure is always transparent and comprehensible to all stakeholders involved.

In addition to assets and processes, risk and measure overview, ibi systems iris also suppoprts you in managing and handling emergency scenarios, business continuity activities and information security events and incidents. Each step can be documented by appropriate evidence (e.g. documents, hints) and used for management reviews, internal and external audits and certifications.



☐	Caption	Created by organization unit	Approval status	Recipients	Priority	Deadline	Progress	Status	Actions
☐	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	ACME Inc.	Decided	John Doe, Jane Doe	High	1/31/2019		Completed	Details ▾
☐	PR.AC-2: Physical access to assets is managed and protected	ACME Inc.	Decided	Jane Doe	High	2/28/2019		Completed	Details ▾
☐	PR.AC-3: Remote access is managed	ACME Inc.	Decided	John Doe, Jane Doe	Medium	2/28/2019		In progress	Details ▾
☐	PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	ACME Inc.	Decided	John Doe	Medium	3/31/2019		In progress	Details ▾
☐	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	ACME Inc.	Decided	John Doe, Jane Doe	Medium	7/31/2019		Open	Details ▾
☐	PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	ACME Inc.	Decided	Jane Doe	High	12/31/2018		Completed	Details ▾
☐	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	ACME Inc.	Decided	Jane Doe	High	12/31/2018		Completed	Details ▾

Derive measures directly from standards like the NIST Cybersecurity Framework and track their implementation status.

Information Security Management System (ISMS) using ibi systems iris

1) Create internal and external regulations, standards and compendia
2) Model architecture (assets and processes) including inheritance of protection requirements
3) Plan and execute assessments as well as reviews for comprehensible documentation
4) Manage findings and implement measures including status monitoring
5) Derive risks, risk treatment options and risk monitorings
6) Manage and handle information security events and incidents
7) Customize workflows and reports and manage relevant documents

ibi systems GmbH
Franz-Mayer-Straße 1
93053 Regensburg
Germany

Contact
phone.: +49 941-462939-0
email: info@ibi-systems.de
www.ibi-systems.de/en