RAM
(Risk Analysis Manager)

Information Security Management System (ISMS) and Risk Management Tool (IRMS)

Use it to create a platform for your security team that Enables easy management and control of assets, risks and related security documentation. With RAM, you can effectively analyze vulnerabilities, risks, plan actions and evaluate both their effectiveness and the state of the systém security management as a whole.

Our team of specialists has been dedicated to the security of information systems for more than 20 years. An integral part of this area is the security of data - primary assets. This is a key issue in all IT products.

We focus mainly on the safety areas defined by ISO 27k standards, ISO 22301, ISO 31000, Act No. 181/2014 Coll. on Cyber Security 253/2008 Coll. on the legalization of proceeds of crime (AML), within the framework which our certified specialists operate.

Information risk management

We can help you implement risk management processes in your organization to remove negative consequencs such as oiverly complex administration, unnecessarily high costs of security. Such processes also help you identify existing vulnerabilities and so resolve them with appropriate and effective measures. We will provide you with the tools for risk management that have been tested in real-life operations.

Information Security Management

We can help you create an information security system in your organization, both in information systems security management and technology implementation, as well as creating security documentation and preparing emergency plans. We will provide you with tools for documentation management, asset management and security implementation measures.

Business Continuity Management

Business continuity management focuses on critical business processes and establishes activities to reduce the risk of a disruptive event. The aim is to protect and preserve the central processes that your organisation needs to function when a disruptive event occurs. We can help you develop a business continuity stratégy and business continuity plans for your key processes. We will provide tools for managing disruptive events and sharing crisis procedures.

Cybersecurity management

We can help you create a cybersecurity management system in your organization according to the applicable legal framework, both in the creation of security documentation and preparation of emergency plans, as well as in the development and operation of your IT. We will provide you with tools for security documentation management, asset management and implementing security measures.

Areas of security:

- **ISO 27k**
- **ISO 22301**
- **ISO 31000**
- **Act no. 181/2014 Coll.**
- **Act no. 253/2008 Coll.**
- **GDPR**

Functionality:

- Custom dial management
- Optional data structure
- Setting the background of items
- Definition of documentation template
- Creation of custom reports
- Setting custom formulas
- Calculations and evaluations
- Dynamic animated charts
- Filter, search, export
- Team outreach

Templates:

- Asset Catalogue
- Threat Catalogue
- Declaration of applicability
- Risk analysis
- Action Plan
- Compliance assessment

Comprehensive dials:

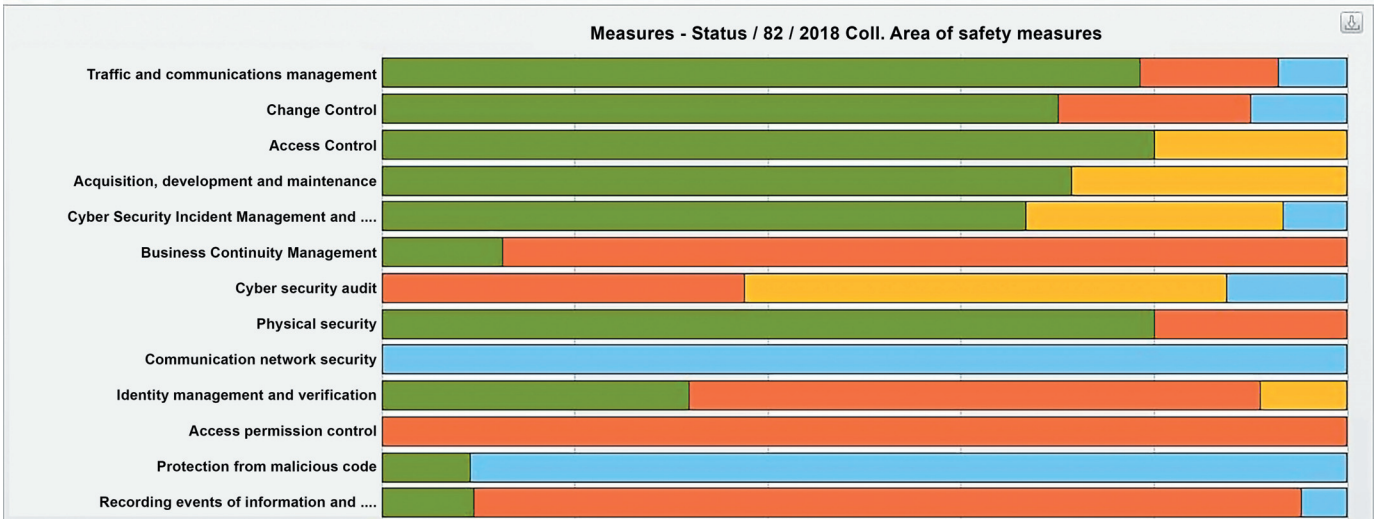
- ISO 27k
- Act No. 181/2014 Coll.
- GDPR GAP
- AML

Individual dials:

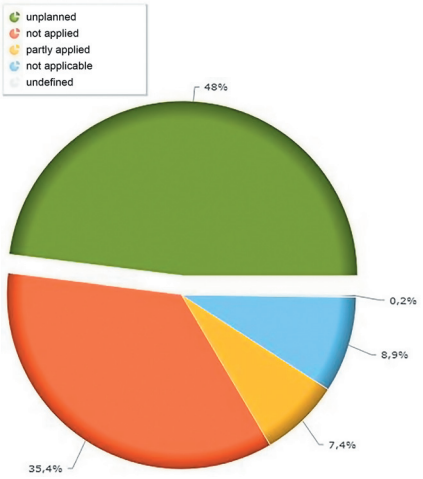
- Confidentiality
- Priority
- Status
- Asset Category
- Asset Availability
- Asset integrity
- Asset value
- Impact level
- Asset Disposal Method
- Reason for processing the asset
- Extent of asset treatment
- Threat level
- Vulnerability level
- Risk level
- Type of threat
- Vulnerability group

PragoData a.s.
www.pragodata.com
Opletalova 1418/23, 110 00 Praha 1
info@pragodata.com

Measures



	Safety precautions	Status	Justification / method of implementation	Documentation
§ 3 a)	establish the scope of the information security management system, taking into account the requirements of the parties concerned and organisational security, identifying the organisational parts and assets covered by the information management systém	applied	Security Policy	SM-BEZP-01
§ 3 b)	sets the objectives of the information security management systém	applied	Security Policy	SM-BEZP-01
§ 3 c)	implement appropriate security measures for the defined scope of the information security management system based on the objectives of the information security management system, security needs and risk assessment	partly applied	BP redesign in progress	
§ 3 d)	manage risks according to § 5	not applied	Unplanned creation of risk management methodology by 11/2018	ISO 3000
§ 3 e)	„establish and approve a security policy in the area of the information security management system, including guiding principles, objectives, security needs, rights and obligations in relation to information security management, and, on the basis of the security needs and the results of the risk assessment, establish a security policy in other areas in accordance with Section 30 and implement appropriate security measures Translated with www.DeepL.com/Translator (free version)“	partly applied	BP redesign in progress	
§ 3 f)	ensure that a cybersecurity audit of the information and communication system is carried out in accordance with § 16	not applied	Not implemented, scheduled for 11 /2018	
§ 3 g)	ensure regular evaluation of the effectiveness of the information security management system, which includes an assessment of the status of the information security management system, including a review of the risk assessment, an assessment of the results of cybersecurity audits conducted and the impact of cybersecurity incidents on the information security management system	not applied	Not carried out, will be implemented on the basis of the 1st audit of the organisation	
§ 3 h)	continuously identify and subsequently manage, in accordance with Section 11, significant changes that fall within the scope of the information security management systém	not applied	Security policy will be updated	



Asset	Risk	Vulnerability	Threat	Impact	Threat	Vulnerabilities	Risk
Economic system (ERP)	R1	Known bugs in programs	Abuse of authorisation	middle	critical	critical	high
LDAP	R2	Not logging events	Abuse of authorisation	high	high	high	high
Personal computer	R3	Alienation	Theft of equipment	middle	low	high	low
Recording studio	R4	Alienation	Theft of equipment	high	low	critical	middle
Printer Minolta TPKC	R5	Fire	Fire	high	low	low	low
Data portal	R6	System upgrade	Data damage	high			
Economic system (ERP)	R7	SW is no longer supported - EOL	Application software malfunctions	middle	critical	middle	middle
Camera system	R8	Risk of vandalism and abuse	Illegal data processing	middle	high	middle	middle

PragoData a.s.
www.pragodata.com
Opletalova 1418/23, 110 00 Praha 1
info@pragodata.com