Consulting • Statistics • IT Solutions • Academy

SERVICE PORTFOLIO

July 2026

risk on mind GmbH
www.riskonmind.eu

Inhalt

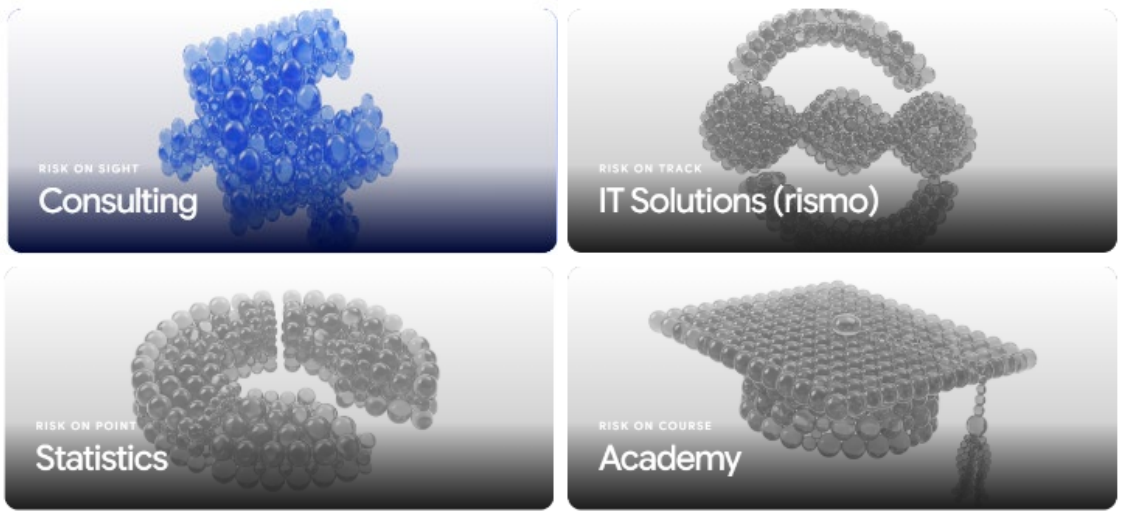
About risk on mind

risk on mind stands for the transformation of risk and compliance requirements from a mere cost factor into a measurable value contribution for companies.

We combine consulting, data, and our software rismo®

- ➔ **Value first:** Every service must create clear economic value
- ➔ **Decision-making:** Decisions are no longer based on gut feelings and assumptions
- ➔ **Economic benefits:** Measurable value contributions for your company
- ➔ **Technical expertise:** We speak the language of insurers, auditors, and technicians
- ➔ **Transparency:** Clear statements on risks, costs, and priorities
- ➔ **Partnership:** Long-term support instead of one-time reports

Service portfolio



Consulting

Risk analysis, assessment, and management of corrective actions. Our consulting services cover the entire risk management cycle.

Risk management

We create transparency for better decisions.

Today, companies face a wide range of risks—from business interruptions and cyberattacks to natural hazards, supply chain disruptions, and increasing insurance requirements. The foundation for effectively managing these risks is an objective understanding of the actual risk situation.

risk on mind conducts a comprehensive analysis of locations, processes, infrastructure, and facilities—both qualitatively and quantitatively. Based on internationally recognized standards such as ISO 31000, ISO 27001, and ONR 49000, we identify and assess both insurable and uninsurable risks. This reveals vulnerabilities, clearly defines priorities, and directs investments where they will have the greatest impact.

Our risk assessment combines decades of practical experience with statistical models and quantitative evaluation methods. This results in transparent decision-making frameworks that take technical, organizational, and economic aspects into account equally. The goal is not maximum security at any cost, but rather the optimal balance between risk and cost.

Building on this, we develop risk-based strategies for avoiding, reducing, transferring, or consciously accepting risks. Companies receive a transparent overview of all available options, including their economic implications—serving as the foundation for well-informed management decisions.

Through continuous monitoring, risks remain visible and manageable even when conditions change. A particular focus is placed on customer training: We empower our customers' employees to independently carry out key activities such as risk identification, internal controls, tracking of measures, documentation, and ongoing assessments in the future. As a result, risk management is not merely viewed as an external project but is permanently embedded within the company. This creates cost transparency, strengthens the company's resilience, and sustainably improves insurability.

With more than 25 years of experience, thousands of risk assessments worldwide, and a unique database, risk on mind helps companies not only manage risks but also turn them into a sustainable competitive advantage.

Your benefits:

- **Objective risk analyses based on international standards:**
  Risks are not assessed based on gut feelings, but rather analyzed in a structured, transparent manner using recognized methods such as ISO 31000, ISO 27001, and ONR 49000. This creates a solid foundation for management decisions, investments, and the further development of the risk strategy.
- **Economically optimized risk management:**
  Measures are prioritized based on risk, impact, feasibility, and cost-benefit ratio. As a result, investments are directed where they make the greatest contribution to risk reduction, business continuity, and long-term value creation.
- **Improved insurability and risk transfer:**
  Transparent risk data, traceable assessments, and effective protective measures strengthen the negotiating position with insurers. At the same time, this creates a solid foundation for long-term insurability, risk transfer, and stable insurance programs.
- **Transparent decision-making criteria for management and owners:**
  Management, owners, and supervisory boards receive clear information about which risks exist, what their impacts are, and which measures make economic sense. This makes risks manageable, allows them to be prioritized, and enables their integration into business decisions.
- **Greater resilience to business disruptions and crises::**
  Critical processes, dependencies, and vulnerabilities become apparent early on. This enables companies to take targeted measures to reduce downtime, shorten recovery times, and ensure their ability to respond in the event of a crisis.
- **Clear prioritization of measures based on risk, impact, and cost-effectiveness:**
  Not every measure offers the same benefit. A structured assessment establishes a clear hierarchy of which measures are necessary in the short term, which should be planned for the medium term, and which are not economically viable.
- **Reduction of unnecessary investments through data-driven decision-making:**
  Risks are assessed both quantitatively and qualitatively. This helps avoid oversized, one-size-fits-all, or ineffective measures and allows budgets to be allocated more effectively. Investments are justified not only on technical grounds but also on economic grounds.
- **Clear and transparent communication with management, owners, insurers, and auditors:**
  The results are presented in a way that clearly explains technical, economic, and underwriting aspects. This facilitates both internal decision-making and external coordination with insurers, auditors, regulatory agencies, and other stakeholders.
- **Early detection of vulnerabilities, dependencies, and critical risk drivers:**
  Locations, processes, facilities, and organizational structures are systematically analyzed. This makes risks visible before they lead to damage, outages, or unexpected costs.
- **Client training and employee empowerment:**
  A key component of sustainable risk management is the targeted training of the client's employees. Since activities such as risk identification, internal controls, self-inspections, tracking of corrective actions, documentation, and ongoing risk assessments are to be carried out by internal employees in the future, their practical training is particularly important. This builds internal expertise, clearly defines responsibilities, and ensures that risk management becomes a permanent part of day-to-day operations.
- **Sustainable Integration into the Company:**
  Through a combination of consulting, methodology, training, and ongoing support,

risk management is not viewed as a one-time report but is established as a repeatable process within the company. Going forward, clients will be able to identify, assess, document, and manage risks more independently.

➔ **Continuous monitoring and sustainable risk management:**
Risks remain visible and manageable even in the face of changing conditions, new locations, modified processes, or increasing requirements. As a result, risk management becomes an ongoing component of corporate governance and supports long-term, resilient business development.

Business Continuity Management (BCM)

We ensure that an incident doesn't bring operations to a standstill.

Crises, fires, cyber incidents, supply chain disruptions, or technical failures cannot always be prevented. What matters most is how quickly a company can respond and restore critical processes. This is exactly where professional Business Continuity Management (BCM) comes into play.

risk on mind supports companies in establishing and further developing business continuity management systems in accordance with international standards such as ISO 22301 and BSI 200-4. The goal is to ensure operational capability even under exceptional conditions and to sustainably reduce the financial impact of disruptions.

As part of Business Impact Analyses (BIA), we examine value chains, business processes, resources, and dependencies in detail. This allows us to identify critical processes, define maximum downtime, and provide transparency regarding the financial consequences of potential business interruptions. This gives companies a solid foundation for strategic decisions and investments in resilience.

Based on these findings, we develop practical emergency, crisis, and recovery plans. This involves evaluating realistic scenarios, establishing recovery strategies, and defining specific measures to maintain business operations even in exceptional situations or to restore them as quickly as possible. The result is a structured BCM system that integrates organizational, technical, and economic requirements.

BCM realizes its full value in an emergency. That is why we also support companies with tests, drills, audits, and preparation for certification according to ISO 22301 or BSI standards. We place a special emphasis on client training: We empower crisis teams, process owners, site managers, and relevant employees to independently carry out BCM tasks in the future. This includes conducting business impact analyses, maintaining emergency and recovery plans, assessing critical dependencies, preparing and conducting drills, and continuously updating BCM documentation. This ensures that plans are not only documented but are also understood, practiced, and can be effectively implemented within the company in the event of an emergency.

With professional business continuity management, risk on mind creates the conditions for resilient companies that remain capable of acting even under difficult conditions, reduce financial losses, and sustainably strengthen the trust of customers, partners, insurers, and employees. By combining consulting, practical customer training, and regular drills, BCM transforms from a theoretical concept into a practical capability within the organization.

Your benefits

- ➔ **Transparency regarding critical processes and dependencies:**
  Business impact analyses systematically identify critical business processes, resources, supply chains, IT systems, key personnel, and external dependencies. This enables companies to recognize which processes are essential for value creation and what the actual impact of a failure would be.
- ➔ **Reduction of business interruption and downtime costs:**
  BCM lays the foundation for detecting disruptions more quickly, limiting their impact, and shortening recovery times. This can significantly reduce financial losses, contractual penalties, delivery failures, and reputational damage.
- ➔ **Structured emergency, crisis, and recovery planning:**
  Emergency plans, crisis management team processes, communication channels, and recovery strategies are clearly defined and tailored to the company's actual requirements. This results in robust guidelines for action in various damage and crisis scenarios.
- ➔ **Client Training and Empowerment of Internal Teams:**
  A central component of our BCM approach is the targeted training of the client's

employees. Crisis teams, process owners, site managers, and key operational personnel learn to independently carry out BCM tasks in the future. This includes business impact analyses, risk and dependency assessments, maintaining emergency plans, tracking measures, documentation, and the preparation and execution of exercises.

- **Practical Exercises Instead of Mere Documentation:**
  BCM plans are only effective if they are regularly tested and understood. Realistic scenarios, tabletop exercises, crisis management team drills, and recovery tests are used to verify whether roles, communication channels, decision-making processes, and technical measures function properly in an emergency.
- **Sustainable integration into the organization:**
  Through a combination of consulting, methodology, training, and practice, BCM is not viewed as a one-time project but is established as a repeatable management process. Internal responsibilities are clearly defined, and employees are empowered to continuously refine the system.
- **Increased organizational resilience:**
  Companies become more resilient to fires, cyber incidents, natural disasters, supply chain disruptions, power outages, and technical failures. Critical processes can be prioritized for protection and restored more quickly in the event of an incident.
- **Improved preparation for audits and certifications:**
  BCM structures, documentation, roles, exercises, and evidence are designed in such a way that they can be presented in a transparent manner to auditors, insurers, government agencies, customers, and certification bodies. This supports, in particular, the requirements of ISO 22301, BSI 200-4, and regulatory resilience requirements.
- **Strengthening trust among customers, partners, and insurers:**
  A transparent and well-rehearsed BCM demonstrates that the company remains capable of operating even in crisis situations. This enhances credibility with customers, suppliers, insurers, banks, owners, and other stakeholders.
- **Sustained protection of corporate value and revenue:**
  Business Continuity Management protects not only individual processes but also the economic performance of the entire company. Through clear recovery strategies, trained teams, and continuous improvement, corporate value, revenue, and market position are secured in the long term.

Versicherungsengineering®

We translate insurance requirements into economically sound decisions.

Insurance requirements are becoming increasingly complex and now extend far beyond the mere purchase of insurance. Requirements imposed by insurers, government agencies, banks, and investors influence investment decisions, technical safeguards, operational processes, new construction and renovation projects, as well as the long-term insurability of companies. However, there is often a lack of transparency regarding which requirements are absolutely necessary, which measures actually reduce risk, and which investments can be justified on economic grounds.

This is precisely where risk on mind's Versicherungsengineering® comes in: We combine technical risk engineering, an understanding of the insurance market, and economic decision-making logic into an integrated consulting approach. The goal is not only to meet insurers' requirements but also to translate them into transparent, prioritized, and economically viable measures.

We analyze locations, processes, buildings, facilities, security systems, and existing insurance programs from both a technical and an underwriting perspective. In doing so, we assess both the actual risk situation and the requirements of the insurance market. Through structured risk analyses, international standards, and decades of practical experience, we determine the actual need for action—prioritized according to risk, effectiveness, cost-effectiveness, feasibility, and acceptance by insurers. The result is a robust basis for decision-making for management, owners, insurers, banks, and other stakeholders.

Our approach prevents companies from blindly adopting blanket lists of measures or making investments whose benefits are not sufficiently substantiated. Instead, we develop realistic and economically viable solutions that balance technical protection, insurability, operational requirements, and investment budgets. This reduces risks, improves protective measures in a targeted manner, and sustainably optimizes the total cost of risk.

A key component of our work is the professional representation of our clients' interests in dealings with insurers, government agencies, banks, and financial institutions. Through data-driven risk assessments, well-founded technical evaluations, and transparent prioritization of measures, we create transparency and facilitate an objective discussion of requirements, conditions, and their actual necessity. This often allows for required investments to be reduced, optimized, staggered over time, or replaced with more effective alternatives without worsening the risk profile.

In addition, we provide comprehensive support for the implementation of protective measures—from detailed technical planning through the bidding process, bid evaluations, and supplier selection to the coordination of all parties involved and successful on-site implementation. In doing so, we ensure that measures are not only planned correctly from a technical standpoint but are also operationally feasible, economically sound, and documented in a manner that is transparent to insurers. This provides companies with a single point of contact for the entire process, from the initial request to effective implementation.

The goal is clear: an improved risk profile, long-term insurability, stable insurance programs, and a reduction in the total cost of risk. At the same time, this results in greater flexibility, increased planning certainty, better investment decisions, and a stronger negotiating position vis-à-vis the insurance market.

With Versicherungsengineering®, risk on mind bridges the gap between risk, technology, insurance, and profitability. Complex insurer requirements are transformed into clear decisions, prioritized measures, and effective protection strategies that safeguard corporate value and strengthen the company's future viability.

Your benefits

- ➔ **Structured Assessment of Insurer Requirements:**
  Insurers' requirements and recommendations are evaluated from technical, economic, and risk-based perspectives. This provides transparency regarding which requirements are absolutely necessary, which measures are negotiable, and which alternatives can achieve the same risk benefits with less effort.
- ➔ **Economic prioritization of investments and measures:**
  Measures are not considered in isolation but are prioritized based on risk impact, protective effect, cost-benefit ratio, feasibility, and insurance relevance. This allows budgets to be allocated strategically where they make the greatest contribution to risk reduction and insurability.
- ➔ **Stronger negotiating position with insurers:**
  Transparent risk data, technical assessments, and clear action plans provide a solid basis for discussions with insurers and reinsurers. Companies can objectively discuss requirements, justify alternatives, and transparently present their risk position.
- ➔ **Support in Negotiations with Government Agencies, Banks, and Investors:**
  Versicherungsengineering® not only supports the dialogue with insurers but also facilitates discussions with government agencies, financiers, owners, and investors. Technical risks, protective measures, and investment needs are presented in a clear and understandable manner and translated into economic decision-making logic.
- ➔ **Improving insurability and risk profile:**
  Targeted protective measures, robust documentation, and transparent risk presentation increase the company's attractiveness to the insurance market. This supports stable insurance capacity, better negotiating leverage, and long-term insurability.
- ➔ **Reduction of the Total Cost of Risk:**
  Not only premiums but also deductibles, claims costs, investments, downtime, internal expenses, and consequential costs are taken into account. This results in a holistic view of the actual risk costs and provides a basis for economically optimized decisions.
- ➔ **Avoiding Unnecessary or Excessive Measures:**
  Required measures are evaluated for their actual impact and cost-effectiveness. This helps avoid excessive investments, develop technical alternatives, or break down measures into manageable implementation phases.
- ➔ **Transparent decision-making criteria for management and owners:**
  Complex technical and underwriting requirements are presented in a way that enables management and owners to make clear decisions. Risks, costs, benefits, priorities, and impacts on insurability are presented in a clear and understandable manner.
- ➔ **Comprehensive support from analysis to implementation:**
  risk on mind supports the entire process—from risk analysis through planning of measures, bidding, and bid evaluation to implementation and documentation. This reduces coordination gaps, clarifies responsibilities, and accelerates implementation.
- ➔ **Improved documentation and evidence management:**
  Insurers, auditors, and stakeholders expect verifiable evidence regarding the risk situation, protective measures, and implementation status. Structured documentation makes requirements verifiable, comparable, and traceable over the long term.
- ➔ **A Sustainable Integration of Technology, Insurance, and Corporate Value:**
  Insurance engineering bridges the gap between technical protection requirements, the insurance market, investment decisions, and corporate strategy. As a result, risks are not only mitigated but also actively managed to safeguard corporate value, resilience, and future viability.

Risk protection concepts

Protection begins before damage occurs—not after.

Today, industrial companies face a wide range of risks: fires, explosions, cyberattacks, natural hazards, supply chain disruptions, power outages, equipment damage, transportation risks, and the failure of critical infrastructure can all cause significant financial and operational impacts in a very short time. Effective protection therefore does not come from individual technical measures, but from a holistic, coordinated risk protection strategy that systematically identifies, prioritizes, and effectively reduces risks.

risk on mind develops integrated protection strategies that combine technical, organizational, operational, and insurance-related requirements. Based on in-depth risk analyses, we assess hazards, identify vulnerabilities, and develop economically optimized protection strategies tailored to the location, industry, risk profile, production processes, and operational conditions

In doing so, we consider not only individual hazards but also a company's entire protection system. Fire protection, explosion protection, cybersecurity, natural hazards, supply chain risks, infrastructure and energy supply, machinery and equipment protection, transportation and logistics risks, and business interruption prevention are integrated into a comprehensive strategy. The result is a set of protective measures that complement one another, have a lasting impact, and simultaneously meet the requirements of insurers, regulatory authorities, owners, investors, and management.

We place particular emphasis on cost-effectiveness and feasibility. Not every measure provides the same benefit, and not every theoretically possible protective measure is practical or economically viable in an operational setting. That is why we evaluate measures based on risk impact, protective effectiveness, priority, investment requirements, operational compatibility, insurance relevance, and cost-benefit ratio. This results in protection concepts that effectively reduce risks, improve insurability, and simultaneously lower the total cost of risk in a sustainable manner.

Existing protective measures are systematically reviewed and optimized. Risks can often be significantly reduced through targeted organizational adjustments, improved maintenance and monitoring processes, clear lines of responsibility, enhanced documentation, or the optimization of existing protective systems—without the need for immediate, large-scale investments. At the same time, transparent strategies provide a solid foundation for insurance negotiations, regulatory proceedings, audit discussions, and investment decisions.

The early integration of protection requirements is particularly crucial for new construction and renovation projects. If fire protection, natural hazards, cybersecurity, supply security, logistics, business interruption prevention, and insurance requirements are taken into account as early as the planning phase, subsequent retrofits, project delays, and unnecessary additional costs can be avoided. risk on mind supports projects from the initial risk assessment through concept development to successful implementation, ensuring that technical protective measures, operational requirements, and insurability are considered together from the very beginning.

From conception to implementation, we coordinate all parties involved, oversee the bidding process, assist with technical decisions, evaluate proposals, and ensure that the defined measures are implemented on schedule, cost-effectively, and in a transparent manner. In doing so, we ensure that security concepts not only work on paper but remain applicable, verifiable, and effective in day-to-day operations.

With customized risk protection strategies, risk on mind lays the foundation for resilient, economically optimized, and long-term insurable business locations. Companies receive a clear roadmap outlining which protective measures are necessary, sensible, and should be prioritized for implementation—and how these can be sustainably integrated into operations, organizational structures, and investment planning.

Your benefits

- ➔ **Comprehensive protection concepts for all relevant risk areas:**
  Risk protection is not viewed in isolation, but rather as an interplay of technical, organizational, operational, and insurance-related measures. This results in a coordinated protection system that takes the company's actual risks into account.
- ➔ **Integration of insurance, regulatory, and operational requirements:**
  Requirements from insurers, regulatory agencies, owners, investors, and day-to-day operations are consolidated at an early stage. This helps avoid conflicting requirements and enables the development of solutions that are technically sound, approvable, and feasible in everyday practice.
- ➔ **Economically optimized protective Mmeasures:**
  Protective measures are evaluated based on risk impact, effectiveness, cost-benefit ratio, feasibility, and insurance relevance. This ensures that investments are targeted precisely where they make the greatest contribution to risk reduction and business continuity.
- ➔ **Improving Resilience and Insurability:**
  Transparent risk management strategies, effective measures, and structured documentation enhance the company's resilience. At the same time, this improves the company's standing with insurers, as risks are presented transparently and actively managed.
- ➔ **Optimizing existing protection structures:**
  Existing protective measures, processes, and responsibilities are systematically reviewed. Often, significant risk reductions can be achieved simply through organizational improvements, better controls, clear lines of responsibility, or the adaptation of existing systems.
- ➔ **Early Involvement in New Construction and Renovation Projects:**
  Security requirements are taken into account as early as the planning phase. This helps avoid costly retrofits, project delays, subsequent insurer requirements, and operational restrictions.
- ➔ **Coordination of implementation through to the final solution:**
  risk on mind supports the implementation process from the concept phase through the bidding process, bid evaluation, and supplier selection to final implementation. This reduces points of interface, ensures sound technical decisions, and ensures that measures are implemented in a transparent manner.
- ➔ **Transparent decision-making criteria for management and owners:**
  Risks, measures, costs, priorities, and impacts on operations and insurability are presented in an easy-to-understand manner. This enables management and owners to make well-informed investment and security decisions.
- ➔ **Strengthening operational implementation and accountability:**
  A protection concept is only effective if it is understood and put into practice within the organization. Therefore, responsibilities, control processes, maintenance requirements, documentation, and internal procedures are clearly defined.
- ➔ **Sustainable reduction of the total cost of risk:**
  Through a combination of loss prevention, targeted investments, improved insurability, reduced downtime, and efficient implementation, the total cost of risk is reduced over the long term.

Our areas of focus

- ➔ **Fire and Explosion Protection:**
  Development of effective protection strategies for fire and explosion risks, including structural, technical, organizational, and insurance-related requirements.
- ➔ **Cybersecurity and Information Security:**
  Integration of cybersecurity and information security risks into the overall protection concept, particularly for critical production processes, IT/OT interfaces, and operational data.
- ➔ **Natural Hazard Management:**
  Assessment of floods, heavy rain, storms, hail, earthquakes, snow loads, and other natural hazards, as well as the development of site-specific protection and preventive measures..
- ➔ **Supply-Chain-Protection:**
  Analysis of critical suppliers, transportation routes, warehousing strategies, and dependencies to better prevent or mitigate delivery failures, bottlenecks, and operational disruptions.
- ➔ **Infrastructure and Energy Supply::**
  Assessment of dependence on electricity, heating, cooling, water, compressed air, gases, communications, and other critical infrastructure, including redundancy and emergency response plans.
- ➔ **Machinery and Equipment Protection:**
  Analysis of critical machinery, production facilities, and technical bottlenecks, as well as the development of protection, maintenance, spare parts, and restart strategies.
- ➔ **Transportation and Logistics Risks:**
  Assessment of warehousing, internal transportation, shipping, transportation routes, and logistics hubs to ensure the flow of goods and delivery capability.
- ➔ **Business Interruption Prevention:**
  Avoiding and minimizing downtime by protecting critical processes, establishing clear recovery strategies, implementing emergency measures, and prioritizing action plans.
- ➔ **Corporate Security and Resilience:**
  Integrating all protective measures into a robust, comprehensive system that safeguards corporate assets, reduces the risk of failure, and strengthens the ability to respond effectively in crisis situations.

Compliance & regulatory resilience

Compliance does not create corporate value—if it is viewed merely as an obligation. When implemented correctly, it becomes a competitive advantage.

Today, companies face a growing number of regulatory requirements that are no longer limited to individual departments. Regulatory resilience is increasingly becoming a management responsibility because laws, guidelines, standards, insurer requirements, customer requirements, and supply chain obligations directly impact business models, investments, processes, and responsibilities. With the CER Directive (Critical Entities Resilience Directive | EU 2022/2557), the European Union has established binding requirements to strengthen the physical and operational resilience of critical entities. The goal is to sustainably improve the resilience of essential services against natural hazards, technical failures, cyberattacks, supply chain disruptions, sabotage, crises, and other threats.

This particularly affects companies in sectors such as energy, transportation, healthcare, drinking water, wastewater, digital infrastructure, finance, public administration, food supply, and other critical sectors. The requirements go well beyond traditional compliance issues. They call for a holistic, all-hazards approach that integrates physical risks, cyber risks, natural hazards, technical failures, supply chain dependencies, personnel availability, crisis management, business continuity management, and documentation.

risk on mind helps companies treat regulatory requirements not merely as a mandatory formality, but as an opportunity to create measurable added value. By combining risk management, business continuity management, information security, risk protection strategies, insurance engineering, and compliance, we develop an integrated approach that equally strengthens resilience, security, insurability, and cost-effectiveness.

As a first step, we analyze which regulatory requirements are relevant to the company and how they relate to existing management systems, risks, processes, and responsibilities. Business impact analyses, risk analyses, gap analyses, maturity assessments, and resilience assessments provide clarity on which areas are critical, what evidence is missing, and which measures yield the greatest benefits for compliance, operational security, and corporate resilience.

Building on this, we develop concrete strategies to build organizational, technical, and regulatory resilience. Emergency and recovery plans, protective measures, crisis management structures, governance processes, responsibilities, control mechanisms, reporting channels, and documentation processes are designed to both meet regulatory requirements and function effectively in day-to-day operations. The goal is not maximum bureaucracy, but an effective system that reduces risks and facilitates decision-making.

There is a particular focus on maintaining a trail of evidence. Regulatory agencies, customers, insurers, auditors, owners, and business partners expect transparent documentation, clear lines of responsibility, regular reviews, and robust evidence of the effectiveness of the measures taken. We help companies implement these requirements in an efficient, structured, and audit-ready manner—from document structure and action plans to evidence of controls, all the way through preparation for regulatory inspections, customer audits, insurer audits, and certifications.

However, regulatory resilience does not arise from documents alone. That is why we also facilitate exercises, tests, simulations, and training sessions to ensure that processes, roles, and responsibilities actually function as intended in an emergency. We place a special emphasis on client training: We empower management, compliance officers, crisis teams, risk owners, process owners, and key operational personnel to understand regulatory requirements, prepare supporting documentation, conduct controls, track measures, and permanently embed resilience requirements within the organization.

With risk on mind, compliance evolves from a regulatory obligation into a strategic tool for resilience, risk reduction, insurability, and sustainable business success. Companies receive not only support in meeting requirements but also a clear roadmap for integrating compliance, risk management, and business continuity into an effective management tool.

Our Services

- **Analysis of Regulatory Requirements::**
  We assess which requirements—including those from CER, NIS2, ISO 27001, ISO 22301, BSI standards, insurer requirements, customer requirements, and other relevant guidelines—are actually applicable to the company. This provides clarity regarding obligations, priorities, and implementation steps.
- **Gap Analysis and Maturity Assessment::**
  Existing processes, documentation, responsibilities, emergency plans, control systems, and evidence are compared against regulatory requirements. This reveals which requirements are already met and where specific action is needed.
- **Risk Analyses Based on the All-Hazards Approach:**
  Physical risks, cyber risks, natural hazards, technical failures, supply chain disruptions, personnel dependencies, and organizational vulnerabilities are considered collectively. This provides a realistic picture of the actual threat landscape and critical dependencies.
- **Business Impact Analyses and Critical Process Assessment:**
  Critical processes, resources, locations, suppliers, IT systems, and infrastructure are analyzed. Companies identify which services are particularly essential for operations, customers, society, or supply capability, and which outages must be prioritized for protection.
- **Establishment of Governance and Compliance Structures:**
  Roles, responsibilities, decision-making pathways, control processes, reporting channels, and escalation mechanisms are clearly defined. This makes compliance manageable and allows it to be permanently integrated into existing management systems.
- **Business Continuity, Emergency, and Crisis Management:**
  We develop or optimize emergency plans, recovery strategies, crisis management team processes, communication structures, and measures to maintain critical services. This ensures that regulatory requirements are aligned with practical operational capabilities.
- **Documentation and Evidence Management:**
  Audit-ready documentation, action plans, evidence of controls, risk overviews, accountability matrices, and reports are structured systematically. This allows requirements to be verifiably demonstrated to authorities, customers, insurers, auditors, and stakeholders.
- **Exercises, Tests, and Resilience Training:**
  Regular exercises, tabletop scenarios, crisis management team drills, recovery tests, and awareness training ensure that processes are not only documented but also function effectively in the event of an incident.
- **Client Training and Empowerment of Internal Teams:**
  We train management, compliance officers, risk owners, crisis response teams, process owners, and operational staff so that regulatory requirements are understood and key activities can be carried out internally in the future. This includes controls, record-keeping, tracking of measures, audit preparation, and ongoing updates to compliance and resilience documentation.
- **Audit and certification preparation:**
  We provide companies with targeted preparation for regulatory inspections, client and insurer audits, and certifications. In this process, documentation, responsibilities, evidence, drills, and the status of measures are organized in such a way that they are verifiable and traceable.

Your benefits

- ➔ **Compliance with regulatory requirements that delivers clear added value:**
  Regulatory requirements are not addressed in isolation but are integrated into existing risk, compliance, security, and resilience processes. This creates a system that meets requirements while simultaneously reducing operational risks.
- ➔ **Transparency regarding obligations, risks, and priorities:**
  Companies gain a clear overview of which requirements are relevant, what gaps exist, and which measures should be implemented first. This facilitates management decisions and prevents unstructured, ad hoc measures.
- ➔ **Greater resilience to crises and disruptions:**
  Critical processes are specifically safeguarded through all-hazards analyses, business impact analyses, emergency planning, and protective measures. Companies can better prevent disruptions, respond more quickly, and maintain essential services for longer periods.
- ➔ **Reduction of operational disruptions and downtime:**
  Critical dependencies, vulnerabilities, and recovery requirements are systematically assessed. This helps reduce downtime, improve recovery strategies, and limit the financial impact of disruptions.
- ➔ **Audit-ready and audit-proof documentation::**
  Evidence is structured in a way that is transparent to authorities, customers, insurers, auditors, and certification bodies. This reduces the audit burden, increases confidence during audits, and strengthens the company's credibility.
- ➔ **Improved insurability and stakeholder confidence:**
  A structured and verifiable resilience and compliance system demonstrates that risks are actively managed. This strengthens the confidence of insurers, customers, banks, owners, investors, and business partners.
- ➔ **Clear Responsibilities and Efficient Governance:**
  Roles, responsibilities, reporting channels, control processes, and escalation procedures are clearly defined. This ensures that regulatory requirements are embedded within the organization and that responsibilities for ongoing implementation are clearly assigned.
- ➔ **Client Training and Internal Capacity Building:**
  Client employees receive targeted training so that they can independently carry out compliance and resilience tasks in the future. This includes controls, tracking measures, maintaining documentation, preparing for audits, conducting risk assessments, and updating supporting documentation..
- ➔ **Sustainable Integration into the Company:**
  Compliance is not viewed as a one-time project but is established as a repeatable management process. Through clear processes, trained employees, regular drills, and ongoing updates, the system remains effective in the long term.
- ➔ **Strategic competitive advantage through regulatory resilience:**
  Companies that integrate compliance, risk management, and business continuity early on can meet requirements more quickly, better demonstrate compliance with customer requirements, ensure delivery capability, and strengthen their position vis-à-vis the market, insurers, and stakeholders.

M&A Due Diligence

The purchase price is rarely the actual risk.

When it comes to corporate acquisitions, real estate portfolios, and industrial investments, the focus is often on financial metrics, market potential, tax issues, and legal considerations. Operational, technical, insurance-related, and resilience-related risks, on the other hand, are often inadequately assessed—even though it is precisely these risks that can lead to significant costs, unplanned investments, business interruptions, limitations on insurability, or impairments after the closing.

risk on mind supports investors, companies, private equity firms, banks, M&A advisors, and industrial groups in identifying and assessing the risks that influence the actual value of an investment. By combining technical risk engineering, insurance engineering, business interruption analysis, natural hazard assessment, risk mitigation strategies, and technical due diligence, we provide transparency regarding factors that often remain hidden in traditional financial or legal due diligence processes.

Our analyses cover buildings, facilities, infrastructure, production processes, energy supply, logistics, fire protection, explosion protection, exposure to natural hazards, technical protection systems, maintenance status, organizational resilience, and existing risk management structures. In addition, we evaluate insurance programs, potential coverage gaps, risk concentrations, deductibles, claims histories, and future insurability requirements. This provides a comprehensive picture of the actual risk situation—not only at the time of the transaction, but throughout the entire life cycle of the investment.

We place particular emphasis on assessing potential business interruption risks, future CAPEX requirements, and value-impacting vulnerabilities. Hidden deficiencies in fire protection, outdated infrastructure, inadequate maintenance strategies, a lack of redundancies, critical supply chain dependencies, or undocumented insurer requirements can have a significant impact on future cash flows, financing, insurability, and enterprise value. Our analyses identify these risks, assess their economic significance, and outline concrete courses of action.

The result is a robust basis for decision-making regarding purchase price negotiations, contract drafting, investment decisions, financing structures, integration strategies, and risk transfer solutions. Buyers gain transparency regarding which risks are being assumed, what immediate and medium-term investment needs exist, what measures are required for insurability, and which risks should be addressed contractually, technically, or organizationally.

However, successful due diligence does not end with the closing. risk on mind also supports companies in the post-merger integration of identified risk, insurance, and protection issues. This includes optimizing insurance programs, harmonizing risk management processes, implementing protection and resilience strategies, prioritizing CAPEX measures, improving maintenance and control structures, and preparing for audits by insurers, regulatory authorities, or customers.

This transforms a transaction into a predictable, controllable, and long-term valuable investment. Risks are not only identified after the purchase but are quantified, prioritized, and integrated into the economic evaluation of the investment even before the decision is made.

Our services

- ➔ **Technical Due Diligence for Industrial and Commercial Sites:**
  Buildings, facilities, infrastructure, production areas, utility systems, and critical operational processes are systematically evaluated. This allows technical vulnerabilities, investment risks, and value-impacting defects to be identified at an early stage.
- ➔ **Risk analyses for buildings, facilities, and infrastructure::**
  We analyze structural, technical, and organizational risks, as well as the condition of relevant protection systems. This analysis also takes into account maintenance, upkeep, redundancies, bottlenecks, and critical dependencies.
- ➔ **Assessment of Natural Hazards and Business Interruption Risks:**
  Locations are assessed for flood, heavy rain, storms, hail, earthquakes, snow load, power outages, and other hazards. At the same time, we analyze the impact that a failure of critical processes would have on revenue, delivery capacity, and enterprise value.
- ➔ **Insurance due diligence and analysis of coverage gaps:**
  Existing insurance programs, deductibles, sublimits, exclusions, claims histories, and insurer requirements are reviewed. This reveals coverage gaps, uninsured risks, and potential limitations on future insurability.
- ➔ **Assessment of protective measures and risk management systems:**
  Fire protection, explosion protection, technical protection systems, organizational controls, internal inspections, emergency plans, and existing risk management processes are reviewed for effectiveness and implementation status.
- ➔ **Analysis of Future Investment and CAPEX Needs::**
  Required investments in protective measures, maintenance, infrastructure, insurability, compliance, or resilience are identified and prioritized. This allows future costs to be realistically factored into the purchase price, financing model, and integration planning.
- ➔ **Risk assessment of portfolios and individual sites:**
  Individual sites and portfolios are evaluated in a comparable manner. This allows for the transparent identification of risk concentrations, particularly critical sites, CAPEX priorities, and priorities for post-merger integration.
- ➔ **Support for purchase price, contract, and risk transfer strategies:**
  The results are prepared in such a way that they can be incorporated into purchase price negotiations, warranties, indemnities, closing conditions, investment planning, and insurance strategies.
- ➔ **Post-merger integration of risk and insurance issues:**
  After closing, we assist with the implementation of identified measures, the harmonization of insurance programs, integration into existing risk management systems, and the prioritization of action plans.
- ➔ **Management-oriented reports and decision-making frameworks:**
  All results are presented clearly, prioritized, and in a financially transparent manner. Management, investors, banks, and owners receive a robust foundation for decision-making before and after the transaction.

Your benefits

- ➔ **Transparency regarding hidden technical and underwriting risks:**
  Risks that are often not sufficiently identified in traditional financial or legal due diligence processes are systematically identified and assessed. This provides buyers with a more realistic picture of the target company's condition, vulnerabilities, and risk exposure.
- ➔ **Realistic assessment of future investment needs:**
  Necessary investments in fire safety, infrastructure, maintenance, resilience, insurability, or compliance are identified early on. This allows CAPEX requirements to

be factored into the purchase price, financing, and integration planning even before closing.

- **Stronger Position in Purchase Price and Contract Negotiations:**
  Technically and economically sound risk assessments provide grounds for purchase price adjustments, warranties, indemnities, closing conditions, or investment commitments. This makes risks negotiable rather than a burden that arises only after the acquisition.
- **Improved Planning Certainty After Closing:**
  Prioritized action plans identify which issues need to be addressed immediately, in the medium term, or in the long term. This allows integration programs, budgets, and responsibilities to be planned early on.
- **Optimized risk transfer and improved insurability:**
  Analyzing existing insurance programs, coverage gaps, and risk mitigation measures creates a solid foundation for restructuring or optimizing insurance coverage after the transaction.
- **Protection of enterprise value and long-term value enhancement:**
  Value-relevant risks are identified early and actively managed. This reduces unexpected costs, business interruptions, insurance restrictions, and reputational damage.
- **Reduction of the Total Cost of Risk:**
  Not only the purchase price and premiums, but also deductibles, claims costs, investments, downtime, internal expenses, and consequential costs are taken into account. This provides a holistic view of the actual risk costs of the investment.
- **Early identification of deal breakers and critical value drivers:**
  Serious technical, underwriting, or resilience-related risks are identified before the contract is signed. At the same time, positive value drivers—such as well-documented protection systems, stable insurability, or strong risk management structures—can be taken into account.
- **Clear priorities for post-merger integration:**
  The results of the due diligence are translated into concrete measures, responsibilities, and implementation priorities. This makes the integration process more structured, faster, and more risk-aware.
- **A robust basis for decision-making for investors, banks, and management:**
  The assessment of technical, operational, and underwriting risks provides certainty for investment committees, financing partners, owners, and management. Decisions are fact-based, transparent, and economically sound.

ESG

Sustainability is becoming a competitive factor—if managed properly.

Environmental, social, and governance (ESG) risks today affect far more than just a company's reputation. They increasingly impact insurability, financing costs, supply chains, regulatory requirements, customer relationships, investment decisions, and long-term competitiveness. Investors, banks, customers, government agencies, and insurers expect transparent information on how companies identify, assess, and manage sustainability, climate, human rights, supply chain, and governance risks.

risk on mind helps companies integrate ESG requirements into existing risk, compliance, and management systems in a pragmatic, risk-based, and economically sound manner. Our goal is not to create additional bureaucracy, but to provide transparency regarding material risks, opportunities, and areas for action. ESG thus becomes an integral part of modern corporate governance—with a clear link to risk management, business continuity management, insurability, financing, and corporate value.

The Corporate Sustainability Reporting Directive (CSRD) and the European Sustainability Reporting Standards (ESRS) introduce extensive requirements for the collection, assessment, documentation, and reporting of sustainability information. The focus is not only on key performance indicators but also on dual materiality: Companies must consider both how their activities impact the environment and society, and how sustainability issues may have financial implications for the company. As a result, ESG becomes a data-driven management task with direct relevance to strategy, risk, investments, and governance.

Our approach integrates ESG with established risk and resilience processes. Environmental, social, and governance risks are systematically identified, assessed, prioritized, and integrated into existing risk management, compliance, business continuity, and insurance processes. These include, in particular, climate risks, natural hazards, energy and resource efficiency, occupational safety, supply chain responsibility, governance structures, compliance, data quality, and record-keeping. This results not in isolated sustainability programs, but in robust decision-making foundations for management, owners, and stakeholders.

In addition to regulatory compliance, the primary focus is on economic benefits. Professional ESG management helps identify financial and operational risks early on, manage investments strategically, optimize energy and resource costs, make supply chains more resilient, increase crisis resilience, and sustainably enhance the company's appeal to customers, investors, banks, insurers, and employees.

Through digital data collection, structured processes, and ongoing adaptation to new regulatory requirements, risk on mind ensures that ESG data can be collected, evaluated, and documented in an efficient, traceable, and auditable manner. Sustainability goals are supported by concrete measures, responsibilities, key performance indicators, and deadlines, and are integrated into operational management. This makes ESG measurable, manageable, and verifiable in a robust manner to both internal and external stakeholders.

We place a special emphasis on customer training and empowering internal teams. ESG can only be effectively implemented over the long term if business units, management, sustainability officers, risk owners, procurement, production, facility management, compliance, and controlling understand the requirements and can carry out key activities independently. We therefore support companies with practical workshops, training sessions, and guided implementation programs to ensure that materiality analyses, data collection, tracking of measures, reporting preparation, and documentation are permanently embedded within the organization. In this way, ESG becomes not a burden, but a tool for resilience, transparency, and long-term value creation.

Our services

- **Integration of ESG Risks into Existing Risk Management Systems:**
  Environmental, social, and governance risks are not considered in isolation but are integrated into existing risk, compliance, BCM, and management processes. This creates a unified management system for sustainability, resilience, and corporate value.
- **Support with CSRD and ESRS Requirements:**
  We provide support for the structured implementation of CSRD and ESRS requirements—from analyzing reporting obligations and data structures to preparing audit-ready documentation. The goal is a practical implementation with as little additional effort as possible.
- **Double Materiality Analysis::**
  We assist companies in assessing impacts, risks, and opportunities according to the principle of double materiality. This involves examining both the company's impacts on the environment and society, as well as the financial impacts of sustainability issues on the company.
- **ESG Risk Analyses and Prioritization:**
  Sustainability risks are systematically identified, assessed, and prioritized. This enables companies to identify which issues are particularly relevant to their strategy, operations, financing, insurability, reputation, and supply chain capabilities.
- **Climate Risk and Resilience Analyses:**
  Physical climate risks such as flooding, heavy rain, heat, storms, hail, or snow load, as well as transitory risks such as regulatory changes, energy prices, or market requirements, are assessed. This leads to concrete measures to strengthen the resilience of locations and the company.
- **Governance and compliance structures:**
  Roles, responsibilities, decision-making processes, control procedures, and reporting requirements are clearly defined. As a result, ESG is not merely reported but embedded in corporate management and existing governance structures.
- **ESG Metrics, Data Collection, and Data Quality:**
  We assist in establishing robust data collection processes, metric systems, and data quality checks. This ensures that ESG information is traceable, comparable, and verifiable.
- **Sustainability and Resilience Strategies:**
  Concrete strategies, goals, measures, and priorities are derived from the results of the analysis. This links ESG to risk reduction, investment planning, insurability, energy efficiency, and long-term corporate development.
- **Audit-Ready Documentation and Reporting Preparation:**
  Reports, supporting documentation, status of measures, responsibilities, and data sources are prepared in such a way that they can be presented in a transparent manner to management, auditors, customers, banks, insurers, and other stakeholders.
- **Client Training and Empowerment of Internal Teams:**
  We train sustainability officers, management, risk owners, functional departments, procurement, production, facility management, compliance, and controlling so that ESG tasks can be understood, managed, and further developed internally in the future. This includes materiality analyses, data collection, tracking of measures, documentation, and preparation for reporting.
- **Linking ESG, BCM, and Risk Management:**
  ESG issues are linked to business continuity management, risk management, natural hazard assessment, compliance, and insurance engineering. This creates an integrated approach that brings together sustainability, resilience, and economic management.

Your benefits

- ➔ **Compliance with regulatory requirements that delivers economic value:**
  CSRD, ESRS, and other ESG requirements are not addressed in isolation but are integrated into existing risk, compliance, and management processes. This creates a system that meets reporting obligations while enabling better decision-making.
- ➔ **Greater transparency regarding sustainability, climate, and governance risks:**
  Significant ESG risks are systematically identified, assessed, and prioritized. Companies recognize which issues may have financial implications and where concrete measures are necessary.
- ➔ **Improved financing opportunities and investor appeal:**
  Transparent ESG data, clear governance structures, and robust sustainability strategies strengthen the trust of banks, investors, and owners. This can facilitate financing discussions and improve access to capital markets.
- ➔ **Strengthening reputation and stakeholder trust:**
  Transparent sustainability information and effective measures demonstrate to customers, employees, suppliers, insurers, and business partners that ESG issues are being actively managed. This enhances the company's credibility.
- ➔ **Reduction of operational and financial risks::**
  Climate risks, supply chain risks, compliance risks, energy dependencies, and governance weaknesses are identified early on. This helps reduce disruptions, cost increases, reputational damage, and regulatory risks.
- ➔ **Integration of sustainability into existing management processes:**
  ESG is not managed as a separate project but is integrated with risk management, BCM, compliance, procurement, production, controlling, and management decisions. This increases effectiveness and reduces additional effort.
- ➔ **Customer training and internal capacity building:**
  The customer's employees receive targeted training so that they can independently carry out ESG tasks in the future. This includes data collection, tracking of measures, materiality analyses, preparation of reports, documentation, and ongoing updates to ESG information.
- ➔ **Audit-Ready Documentation and Improved Traceability:**
  ESG data, processes, measures, and responsibilities are documented in a way that is transparent to management, auditors, customers, banks, insurers, and regulatory authorities. This reduces the audit burden and increases confidence in audit results.
- ➔ **Better management of initiatives and investments:**
  ESG goals are linked to specific initiatives, responsibilities, metrics, and priorities. This allows investments to be targeted where they make the greatest contribution to risk reduction, resilience, and value creation.
- ➔ **Sustainable increase in resilience and corporate value:**
  By integrating ESG, risk management, business continuity, and governance, sustainability becomes a tool for long-term competitiveness. Companies become more resilient, more transparent, and better prepared for future challenges.

NIS2 / CER / ISO 27001

Resilience, information security, and compliance are becoming management responsibilities.

With the NIS2 Directive, the CER Directive, and international standards such as ISO/IEC 27001, the demands on companies to holistically manage cybersecurity, operational resilience, and information security are increasing. NIS2 extends cybersecurity requirements to numerous critical and important sectors and requires appropriate technical, organizational, and operational measures to manage risks to network and information systems. The CER Directive complements this approach by addressing the physical and organizational resilience of critical infrastructure against all relevant threats. ISO/IEC 27001 provides the internationally recognized framework for a risk-based information security management system.

This is no longer just about IT security or formal compliance with regulatory requirements. What is required are robust management systems, clear responsibilities, effective controls, verifiable risk assessments, functioning reporting and escalation channels, and structured emergency and crisis management. Cyber risks, physical risks, supply chain dependencies, critical processes, staff availability, service provider management, and business interruptions must be considered collectively.

risk on mind helps companies treat NIS2, CER, and ISO 27001 not as separate, parallel requirements, but rather to integrate them into a unified approach to resilience and information security. Our approach combines information security, business continuity management, risk management, compliance, physical security, supply chain resilience, and insurability into a practical system that meets regulatory requirements while simultaneously creating measurable added value for the company.

As part of our analyses, we examine critical processes, information, assets, locations, IT and OT systems, service providers, supply chains, infrastructure, and organizational dependencies using the all-hazards approach. This not only reveals cyber risks but also identifies vulnerabilities in buildings, energy supply, emergency response organization, crisis communication, recovery planning, supplier management, and physical security. The results form the basis for targeted measures that reduce risks, limit downtime, and strengthen the company's ability to respond effectively.

Based on structured risk analyses, business impact analyses, gap analyses, and maturity assessments, we develop security, emergency, recovery, and resilience plans that meet both legal requirements and the practical needs of the business. Governance structures, responsibilities, reporting processes, control mechanisms, risk treatment plans, supplier requirements, awareness initiatives, and technical safeguards are designed to function effectively in day-to-day operations and to be effective in the event of an incident.

In addition, we support companies with exercises, tests, training sessions, and awareness programs to ensure that processes and responsibilities are not only documented but are actually understood and applied. A particular focus is placed on customer training: We empower management, information security officers, risk owners, IT and OT managers, crisis response teams, process owners, and key operational personnel to independently carry out core activities in the future. These include risk analyses, control activities, tracking of measures, incident preparedness, audit preparation, documentation maintenance, and the ongoing development of the ISMS and resilience processes.

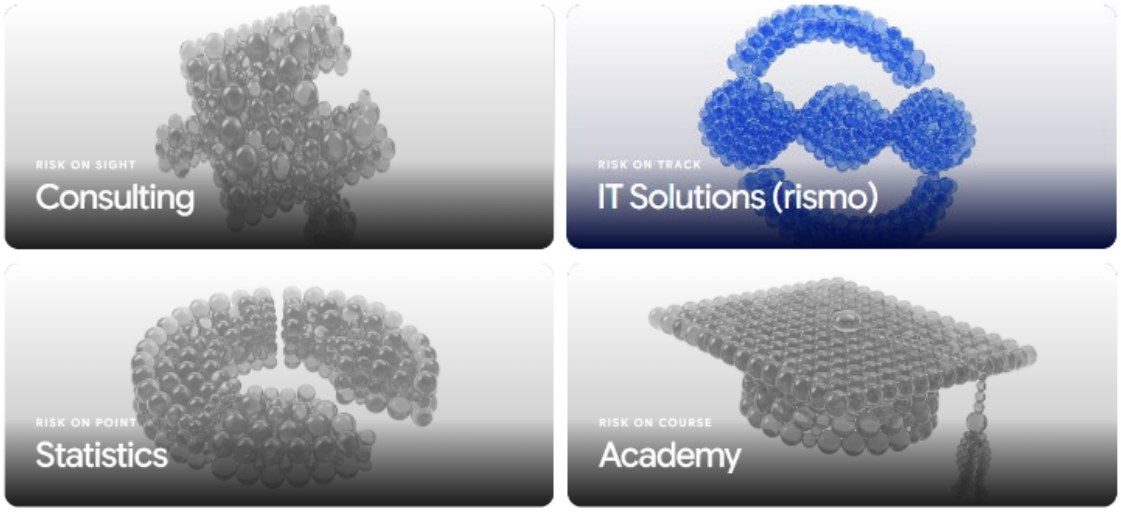
With risk-on mind, NIS2, CER, and ISO 27001 become not a burden but an opportunity to reduce risks, build resilience, improve insurability, and sustainably strengthen the company's future viability. Regulatory requirements give rise to clear responsibilities, robust processes, better decision-making foundations, and an effective management system for cybersecurity, information security, and operational resilience.

Our services

- **NIS2 Readiness Assessments:**
  We assess whether and to what extent companies are affected by NIS2, which requirements are already being met, and where action is needed. In doing so, we examine governance, risk management, incident handling, business continuity, supply chain security, cyber hygiene, awareness, access control, and reporting processes.
- **CER and Resilience Analyses Based on the All-Hazards Approach:**
  We assess the resilience of critical processes, locations, infrastructure, and services against cyber incidents, natural hazards, technical failures, physical threats, supply chain disruptions, and organizational dependencies.
- **ISO 27001 Implementation and ISMS Development:**
  We provide support in establishing, further developing, and preparing for audits of an information security management system. This includes scope definition, risk analysis, risk treatment, the Statement of Applicability, security policies, control implementation, internal audits, and management reviews.
- **Risk Analyses and Business Impact Analyses:**
  Critical information, systems, processes, locations, service providers, and dependencies are assessed. This reveals which failures would have a particularly significant impact and which protective and recovery measures must be prioritized.
- **Information Security Management Systems and Risk Treatment:**
  Risks to the confidentiality, integrity, and availability of information are systematically identified, assessed, and addressed. Measures are prioritized, responsibilities are defined, and controls are documented in a traceable manner.
- **Business Continuity, Emergency and Crisis Management:**
  We develop emergency plans, recovery strategies, communication processes, crisis management team structures, and decision-making pathways. This ensures that NIS2, CER, and ISO 27001 requirements are combined with practical operational capabilities.
- **Governance and Compliance Structures:**
  Roles, responsibilities, reporting channels, escalation processes, control mechanisms, and management reports are clearly defined. This ensures that information security is not only implemented technically but is also embedded as a leadership and management responsibility.
- **Supply Chain and Service Provider Management:**
  Direct suppliers, IT service providers, cloud providers, maintenance companies, and critical outsourcing partners are included in the risk assessment. This allows for better management of dependencies, vulnerabilities, and contractual security requirements.
- **Exercises, Tests, and Awareness Training:**
  Tabletop exercises, incident simulations, crisis management team exercises, recovery tests, and awareness training ensure that processes, roles, and reporting channels function properly in an emergency and are understood by employees.
- **Customer Training and Empowerment of Internal Teams:**
- We train management, information security officers, risk owners, IT and OT managers, crisis teams, and process owners. The goal is to enable the organization to conduct risk analyses, control activities, track measures, prepare for incidents, prepare for audits, and maintain documentation internally in the future.
- **Audit-ready documentation and evidence management:**
  Risk registers, action plans, guidelines, evidence of controls, audit documents, management reports, and evidence of effectiveness are structured systematically. This ensures that requirements set by regulatory authorities, customers, insurers, auditors, and stakeholders can be verifiably documented.

Your benefits

- **Compliance with regulatory requirements with integrated added value::**
  NIS2, CER, and ISO 27001 are not considered in isolation but are integrated into a unified management system for information security, resilience, and risk management. This ensures that requirements are met efficiently while simultaneously reducing operational risks.
- **Greater cyber and business resilience:**
  Cybersecurity, physical security, business continuity, supply chain resilience, and crisis management are considered holistically. Companies can better prevent incidents, respond more quickly, and maintain critical services for longer periods.
- **Clear management accountability and governance:**
  Roles, responsibilities, decision-making processes, reporting procedures, and control mechanisms are clearly defined. This makes information security a transparent management responsibility rather than merely a technical IT issue.
- **Reduction of business interruptions and security risks:**
  Critical processes, systems, information, locations, and service providers are assessed on a risk-based basis. This leads to targeted measures to reduce downtime, shorten recovery times, and limit the impact of security incidents.
- **Transparent and auditable documentation:**
  Risk assessments, measures, controls, policies, responsibilities, and evidence are documented in a way that allows them to be verified by regulatory authorities, customers, insurers, auditors, and certification bodies.
- **Improved insurability and stakeholder trust:**
  A robust information security and resilience system demonstrates that cyber and operational risks are actively managed. This strengthens the organization's position with insurers, customers, banks, owners, investors, and business partners.
- **Better management of supply chain and service provider risks:**
  Dependencies on IT service providers, cloud providers, maintenance firms, suppliers, and outsourcing partners become visible and manageable. This allows security requirements to be defined more clearly and risks along the value chain to be reduced.
- **Customer training and internal capacity building:**
  The customer's employees receive targeted training so that key tasks can be performed internally in the future. These include risk analyses, control activities, tracking of measures, incident preparedness, audit preparation, documentation maintenance, and the ongoing development of the ISMS.
- **Sustainable strengthening of business and delivery capabilities:**
  By combining information security, business continuity, and operational resilience, critical services remain more readily available even during disruptions. This improves delivery capabilities, customer trust, and economic stability.
- **Economically sound implementation rather than mere compliance:**
  Measures are prioritized based on risk, impact, feasibility, and cost-benefit ratio. This avoids creating a bureaucratic side project and instead establishes an effective system for managing cyber, information security, and resilience risks.



IT-Solutions

rismo® – The digital platform for data-driven risk management, action planning, and management decisions.

rismo® brings clarity to areas where risk assessments in many companies are still shaped by individual opinions, anecdotal evidence, or inconsistent evaluations. The platform consolidates risk data, location information, questionnaires, assessments, measures, documentation, and reports into a single, centralized digital environment. This creates an objective, standardized, and fully traceable picture of the risk situation at all times.

Subjective assessments are replaced by structured, data-driven risk assessments. rismo® uses statistical risk data, location-specific information, company-specific details, and AI-powered analyses to make risks comparable, prioritizable, and manageable. The results are presented transparently in risk overviews, heat maps, action lists, and reports, thereby supporting decisions at the operational, tactical, and strategic levels.

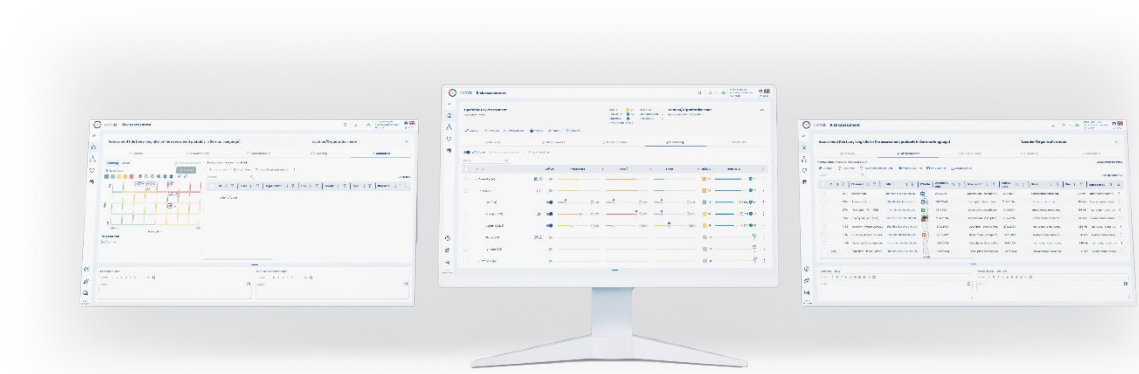
The platform combines risk management, insurance engineering, business continuity, compliance, ESG, NIS2/CER requirements, and site assessments into a single integrated system. This provides companies not only with a digital registry but also with an active management tool for risks, measures, responsibilities, and documentation. rismo® delivers comparability, transparency, and speed—especially for organizations with multiple locations, international operations, or complex risk profiles.

A key advantage lies in the combination of software and specialized methodology. rismo® does more than just map data; it helps companies systematically identify and assess risks, derive mitigation measures, and track their implementation. This transforms risk management from a static report into an ongoing, data-driven management process.

- ➔ **Centralized database for all risks:**
  All relevant risk information, location data, assessments, measures, documentation, and responsibilities are managed on a single platform. This ensures that information is not lost in individual files, emails, or local lists.
- ➔ **Automated Analyses and Reports:**
  rismo® supports the automated evaluation of risk data and generates structured reports for management, insurers, auditors, and internal stakeholders. This reduces manual effort and improves the quality of the information used to make decisions.
- ➔ **Action Management and Tracking:**
  Actions can be derived directly from assessments, assigned to responsible parties, and

given deadlines. The implementation status remains visible at all times, supporting consistent tracking.

- **Documentation and Evidence Management:**
  Evidence, comments, photos, documents, and implementation information can be stored centrally. This creates traceable documentation for audits, insurers, regulatory agencies, management, and internal controls.
- **Support through AI and Automation:**
  AI-powered analyses help classify risks more quickly, highlight deviations, and identify priorities. Automation supports standardization and reduces subjective bias.
- **Comparability Across Locations and Organizational Units:**
  Risks, protection levels, status of measures, and maturity levels can be compared across multiple locations. This reveals risk concentrations, vulnerabilities, and best-practice locations.
- **Digital foundation for sustainable risk management:**
  rismo® provides the technical foundation for permanently embedding risk management within the company and continuously developing it further.



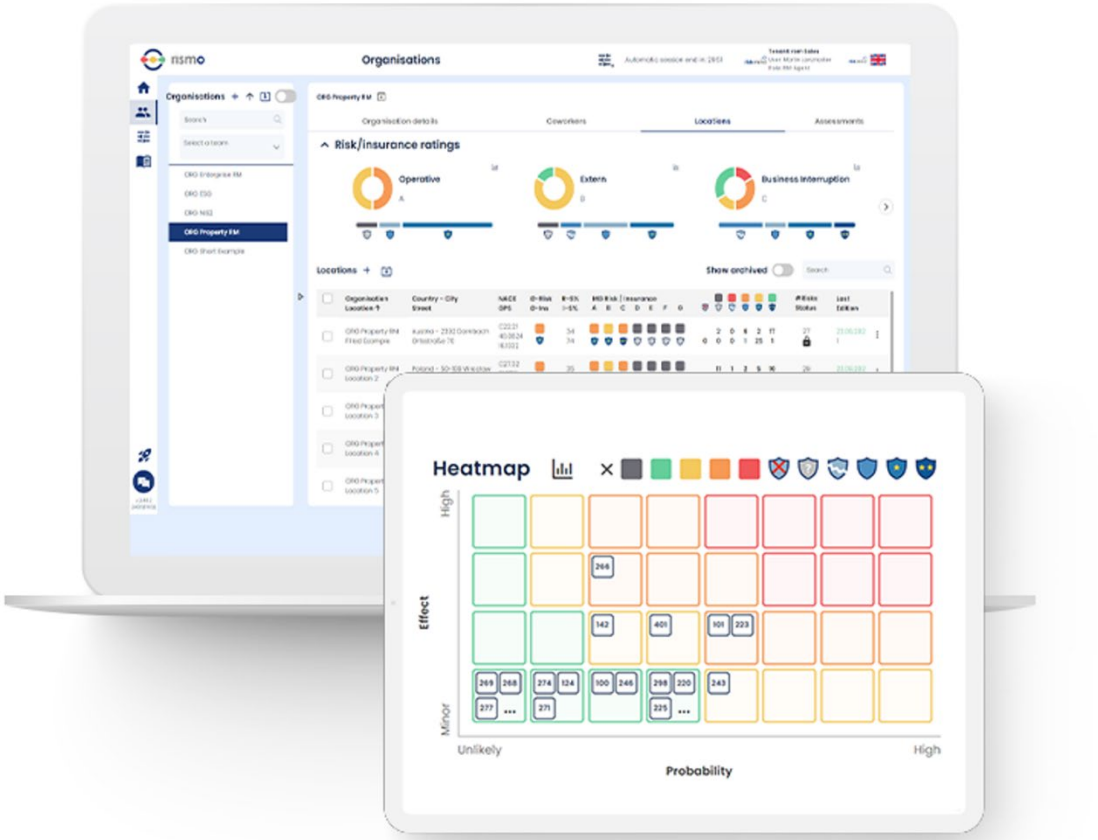
How does rismo® work?

- **Step 1**
  Custom Data Collection & Risk Analysis with AI
  Operating mode, location data, and GPS coordinates are entered or imported in a structured format. rismo® links this information with statistical risk data, industry-specific hazard profiles, and location-based parameters. This quickly generates an initial data-driven hazard assessment that is significantly more reliable than a purely subjective initial assessment.

- **Step 2**
  Risk Assessment with AI & Targeted Risk Management
  rismo® provides structured questionnaires for risk owners, site managers, or specialized departments and, based on the responses, evaluates whether the individual level of protection is better or worse than the statistical baseline risk. The result is a comprehensive risk assessment featuring AI-supported evaluation, standardized methodology, and transparent presentation in risk overviews and heat maps in accordance with ISO 31000.

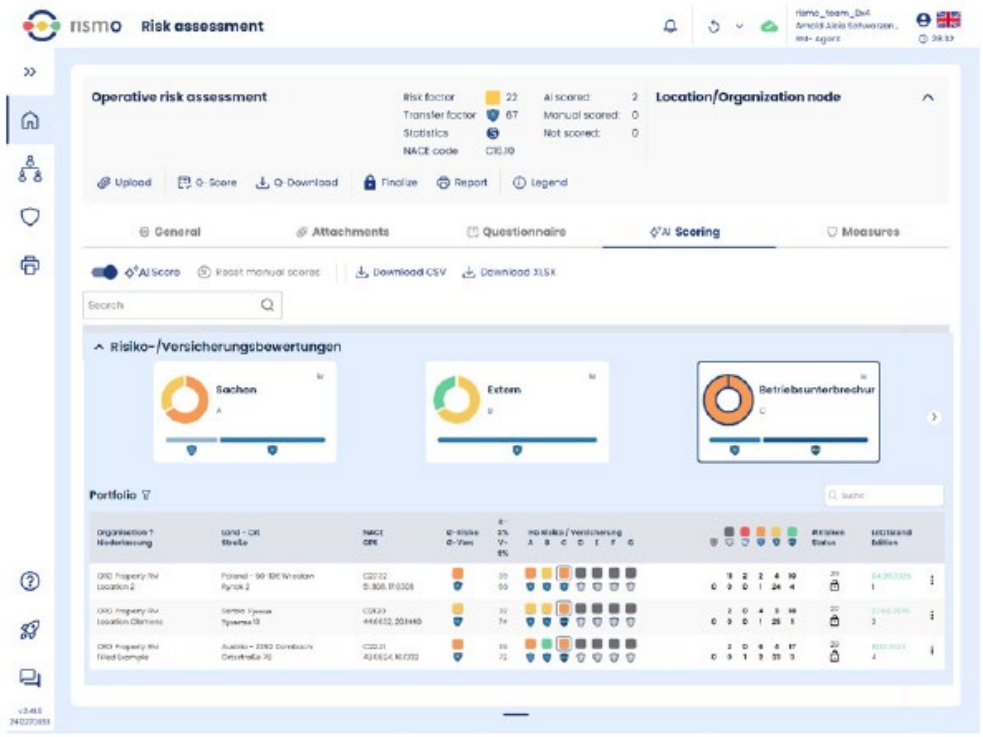
➔ **Step 3**
Take Action – Define and Manage Measures
Based on the assessments, specific measures can be identified, responsibilities assigned, deadlines set, and implementation progress tracked. Management, insurers, auditors, and internal stakeholders automatically receive structured reports that show which risks exist, what measures are necessary, and how far implementation has progressed.

This creates a closed-loop risk management cycle: risks are identified, assessed, prioritized, translated into actions, monitored, and regularly updated. As a result, companies can track at any time how their risk profile is evolving and which issues require special management attention.



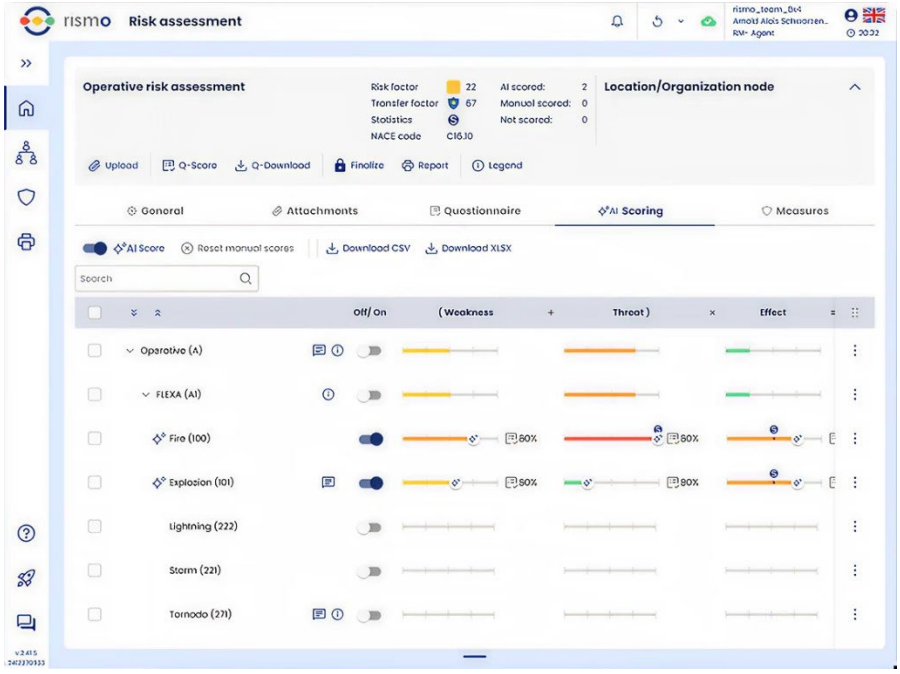
Features

- **AI Analytics:**
  rismo® automatically classifies risks—based on statistical risk data, company-specific information, and structured questionnaires. The result is an objective AI score that makes risks comparable across locations, business units, and time periods.
- **Risk heat map according to ISO 31000:**
  All material risks are presented according to likelihood of occurrence, impact, and degree of protection. Critical risks are immediately identifiable, filterable, and prioritizable. This enables management and functional departments to decide more quickly which measures should be implemented first.
- **Customizable without coding:**
  Risks, questionnaires, assessment criteria, control activities, and risk categories can be flexibly customized. Companies can map industry-specific requirements, internal standards, or insurer requirements without needing to develop their own software.
- **Multi-site management:**
  Whether there are five sites or several hundred—rismo® enables consistent assessment, control, and tracking across the entire organization. This provides transparency regarding site comparisons, risk concentrations, the status of measures, and best practices.
- **Detailed Reporting:**
  Reports for management, insurers, the supervisory board, auditors, or internal departments are generated based on existing data. This reduces manual effort, improves traceability, and provides a consistent basis for decision-making.
- **Action and Responsibility Management:**
  Recommendations and actions can be recorded, prioritized, and assigned to responsible parties directly within the system. Deadlines, statuses, comments, and supporting documentation remain clearly documented and traceable.
- **Document and Evidence Management:**
  Comments, photos, inspection reports, maintenance records, audit documents, and other files can be stored directly alongside risks, actions, or locations. This significantly simplifies the process of providing evidence to insurers, auditors, and management.
- **Recognition and Clarity for Insurers:**
  Through standardized methodology, transparent assessment, and traceable reports, rismo® supports professional dialogue with insurers. Risk positions and improvement measures can be presented and negotiated more clearly.
- **Scalable platform for risk management, compliance, and resilience:**
  rismo® can be used as a digital foundation for a variety of risk areas—from traditional industrial risks to BCM and insurance engineering, as well as compliance, ESG, NIS2/CER, and audit preparation.



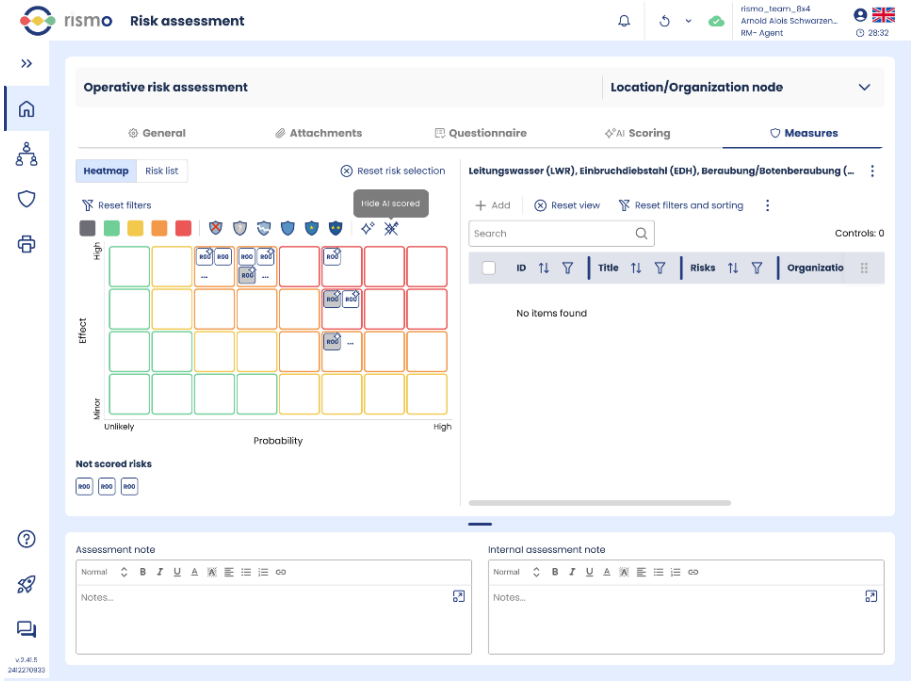
Statistics as the Foundation for Objective Decisions

risk on mind has an extensive collection of statistical risk data from projects, loss analyses, risk assessments, and insurance engineering. rismo® uses this depth of data as a basis for evaluating risks not in isolation, but in comparison to the industry, location, type of operation, and level of protection.



No coding knowledge required

Adjust the scope of risk data, add new risks, change assessment criteria, or define control activities—all of this can be done directly within the interface. This ensures that business units remain operational and do not have to wait for external development or internal IT resources for every adjustment.

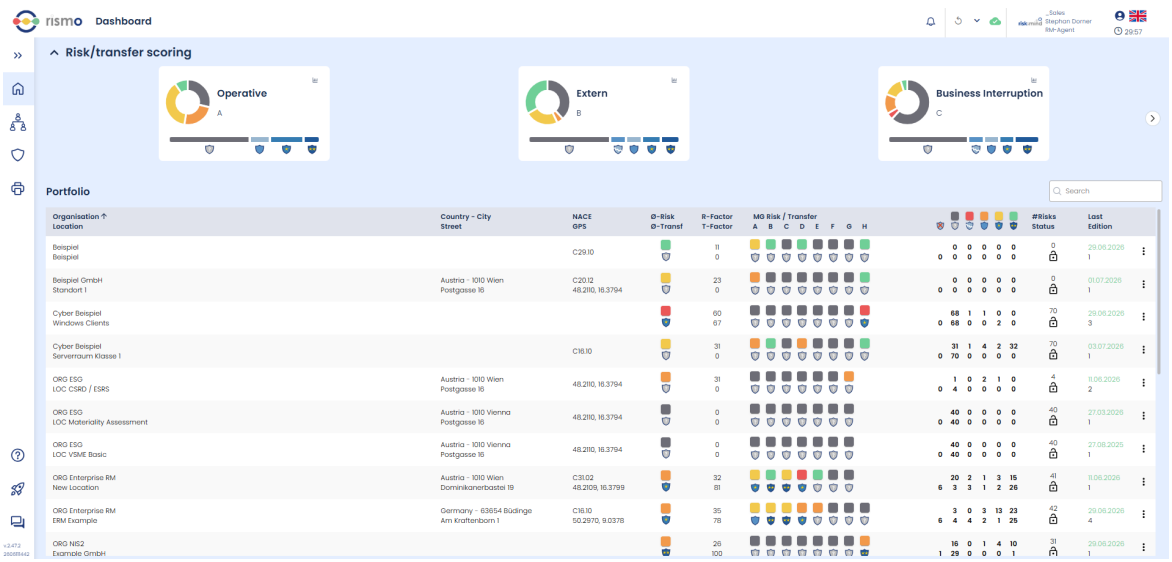


Intuitive and Well-Organized

rismo® is designed so that risk managers, site managers, functional departments, and management can quickly get up to speed with the platform. Clear structures, easy-to-understand dashboards, and transparent workflows ensure that risk management becomes simpler, not more complicated.

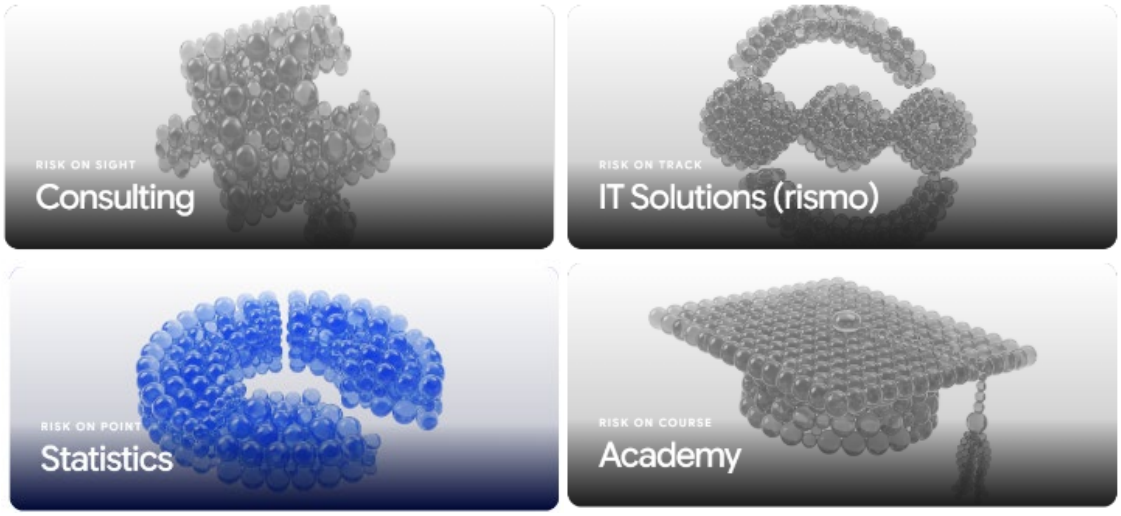
The Core Promise:

Risk assessments that do not depend on personal experience, individual judgments, or inconsistent evaluation standards, but rather on data, methodology, and transparent criteria. rismo® makes risks comparable, reproducible, and robust—thereby laying the foundation for better management decisions, more effective measures, and a stronger negotiating position with insurers and stakeholders.



Many additional features for risk assessment, site management, action tracking, documentation, audit preparation, reporting, and continuous monitoring.

See rismo in action: You can find all current training sessions on [our website]():



Statistics

Data creates transparency. Knowledge creates competitive advantages.

Risk management is only as good as the data on which decisions are based. That is why risk on mind combines decades of practical experience with an extensive database of claims, risk assessments, insurance analyses, natural hazard assessments, business interruption analyses, industry comparisons, and international best-practice standards.

Our Risk Intelligence methodology distills a large number of data points into understandable, reliable, and economically actionable decision-making foundations. This provides companies not only with insights into their own risk profile but also with an objective comparison to typical loss patterns, industry-specific hazards, regional natural hazards, technical vulnerabilities, and developments in the international insurance market.

The result is fact-based decisions rather than assumptions. Risks are not merely described but evaluated in terms of probability of occurrence, extent of loss, business interruption impact, insurability, and economic relevance. This creates a robust foundation for investment decisions, prioritization of measures, insurance negotiations, and strategic risk management.

Statistics thus serve as a bridge between technical risk analysis and business decision-making. They reveal which risks are actually relevant, which measures make economic sense, and where investments contribute most to risk reduction, resilience, and insurability.

What we provide:

- ➔ **Claim frequencies by industry and business type:**
  We analyze how frequently certain loss events occur across different industries. This enables companies to better assess whether a risk is merely theoretical or statistically significant. Examples include fires at wood-processing facilities, machinery breakdowns in metal fabrication, exposure to natural hazards at industrial sites, or typical business interruptions in complex supply chains.
- ➔ **Maximum loss scenarios and economic impacts:**
  We assess the potential financial consequences of a realistic major loss. This analysis takes into account property damage, business interruption, restart times, supply obligations, market losses, additional costs, tax implications, and potential limitations on insurability.
- ➔ **Quantitative Risk Analyses::**
  Risks are not only described qualitatively but are also quantitatively assessed based on statistical models, historical loss patterns, and company-specific parameters. This

provides companies with a reliable estimate of the risk costs that can realistically be expected over a defined period.

- ➔ **Industry-Specific Risk Profiles:**
  Typical hazards, loss frequencies, loss magnitudes, and protection requirements are presented in a structured manner for different types of operations. This provides a quick and transparent overview of which risks are particularly relevant to a given industry and which protective measures typically yield the greatest benefits.
- ➔ **Data-Driven Decision-Making for Management and Owners:**
  Management and owners need numbers, priorities, and economic justifications. Our analyses translate technical risks into clear, actionable insights for investment decisions, insurance strategies, CAPEX planning, risk transfer, and prioritizing measures.
- ➔ **Statistical trend analyses:**
  We analyze how risks evolve over time. Increasing claim frequencies, new hazards, changing insurer requirements, climate trends, or changes in supply chains become apparent and can be integrated into risk management at an early stage.
- ➔ **Benchmarking and Comparability:**
  Companies can compare their risk profile with industry-specific empirical data, comparable locations, and international best practices. This reveals whether a location is better, worse, or averagely protected and which improvements deliver the greatest added value.

How we obtain relevant risk data

The quality of a risk analysis depends directly on the quality, timeliness, and relevance of the underlying data. That is why risk on mind uses various data sources, evaluates their validity, and combines them using a structured process. Only by combining internal company data, external risk data, and our own project experience can we create a reliable picture of the actual risk situation.

Internal Company Data

- Production and operational data for assessing critical processes, capacities, and bottlenecks
- Claim histories and incident reports for identifying recurring patterns and vulnerabilities
- Maintenance and repair data for assessing technical reliability and failure probabilities
- Emergency, crisis, and restart documentation to assess organizational resilience
- Insurance information, coverage structures, deductibles, and insurer requirements
- Business interruption data, supply obligations, revenue contributions, and restart times

External risk data

- International loss statistics and industrial loss data
- Insurance and market analyses on capacity, premium trends, and underwriting appetite
- Natural hazard models for floods, heavy rain, storms, hail, earthquakes, snow load, and other hazards
- Weather, climate, and geodata for assessing location-specific exposures
- Supply chain, industry, and market data for assessing external dependencies
- Industry benchmarks and international best practices for classifying individual risk levels

Proprietary Database

- Thousands of risk inspections and site assessments worldwide
- International industry audits across various sectors and risk classes
- Insurance engineering projects focusing on protective measures, insurability, and total cost of risk
- BCM, risk management, compliance, and resilience projects
- Analysis of actual claims and typical causes of loss

- Assessment of the economic impact of property damage, business interruptions, and risk concentrations

Combining this data provides an objective and transparent picture of a company's actual risk profile. Risks are not considered in isolation but are assessed in relation to the industry, location, level of protection, claims history, potential for business interruption, and insurability.

Basic Statistical Data on Industrial Risks

Understanding Risks Before They Cause Damage

Our database contains structured information on the most important risk areas for industrial companies. This data helps assess probabilities of occurrence, potential extent of damage, typical vulnerabilities, protection requirements, and economic impacts.

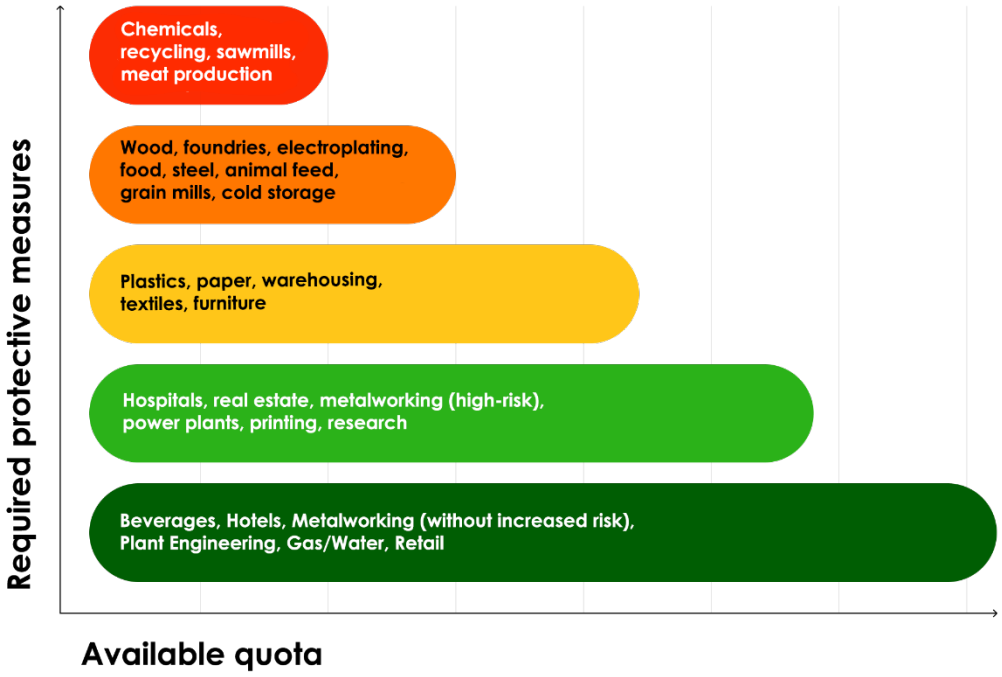
- Fire and explosion risks, including typical causes of damage, fire loads, protection systems, and propagation scenarios
- Business interruptions, with a focus on critical processes, restart times, bottlenecks, and financial impacts
- Natural hazards such as flooding, heavy rain, storms, hail, earthquakes, snow loads, and climate-related changes
- Machinery and equipment failures, including technical bottlenecks, spare parts availability, and maintenance quality
- Cyber risks related to information security, IT/OT dependencies, downtime, and recovery
- Logistics and supply chain disruptions involving critical suppliers, transportation routes, warehousing strategies, and customer obligations
- Infrastructure and energy outages, including electricity, heating, cooling, water, compressed air, gases, and communications
- Environmental, compliance, and regulatory risks related to government requirements, ESG, NIS2, CER, and insurability

Statistics – the foundation for informed risk decisions

When senior management or the CFO asks how likely a significant loss is, what level of loss can realistically be expected, and what investment makes economic sense, many companies lack reliable answers. The reason is often an inadequate data set or an assessment based more on experience and individual opinions than on verifiable figures.

risk on mind bridges this gap with statistical analyses of loss frequencies, loss magnitudes, risk drivers, industry profiles, location exposures, and risk trends. These analyses provide a solid foundation for decisions regarding risk, investment, insurance, and resilience.

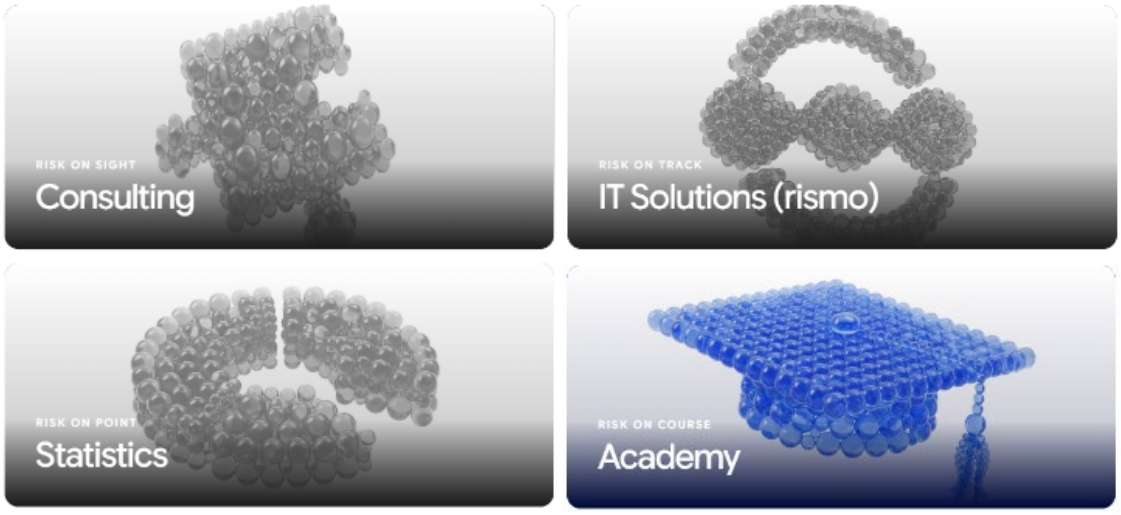
Industry, type of operation, location, level of protection, and loss history determine how risks are assessed, which measures make economic sense, and how the insurance market evaluates a company. The decisive factor remains the same in every risk class: a verifiably managed risk based on reliable data.



Risk Intelligence made by risk on mind

Data leads to decisions. Decisions lead to resilience.

With our unique combination of claims statistics, insurance expertise, industrial risk management practices, digital analytical methods, and rismo®, we lay the foundation for well-informed decisions in an increasingly uncertain world. Companies can identify earlier which risks are material, which measures are effective, and how investments in risk reduction, insurability, and resilience can be justified from a financial perspective.



Academy

Knowledge builds resilience. Education provides security. Competence enables action.

Modern industrial companies face increasingly complex challenges: Insurers expect demonstrable risk management expertise, regulatory agencies are tightening requirements, and at the same time, risks are rising due to cyberattacks, business interruptions, natural hazards, technical failures, supply chain disruptions, and organizational dependencies. Sustainable protection for a company therefore begins not solely with technical safeguards, but with the people who must identify, assess, document, and manage risks in their day-to-day work.

The risk on mind Academy provides practical knowledge on risk management, fire safety, business continuity management, cybersecurity, information security, compliance, insurance requirements, and corporate resilience. Our training programs are based on international standards, real-world claims, industry best practices, and decades of experience gained from thousands of risk assessments worldwide. As a result, participants gain not only theoretical knowledge but also concrete tools for daily application within their organizations.

The goal is to empower employees, managers, risk owners, fire safety officers, crisis response teams, site managers, and key operational personnel to identify risks early on, assess them correctly, and independently implement effective measures. The focus is not on theoretical standards, but on practical applicability in everyday industrial settings: conducting self-inspections, identifying deviations, tracking measures, maintaining documentation, preparing for audits, and responding correctly in the event of an incident.

The Academy combines training, certification, practical exercises, and continuous professional development into a modular system that makes companies more resilient in the long term while also supporting insurance, audit, and compliance requirements. Companies benefit from internal expertise, clear responsibilities, and a stronger risk culture. As a result, core activities are not permanently outsourced to external consultants but are gradually embedded within the company.

Our training programs are deliberately designed to be practical: case studies, real-life loss events, checklists, site inspection procedures, group work, scenario-based exercises, and concrete implementation guides ensure that what is learned can be applied immediately. Participants not only learn to understand requirements but also to translate them into concrete actions, controls, and improvement measures.

This makes continuing education a strategic component of risk management: it reduces dependencies, accelerates implementation, improves the quality of internal controls, and

creates a solid foundation for discussions with insurers, auditors, regulatory authorities, customers, and management.

Our training programs

Fire safety: self-checks & self-inspection

Online Training | approx. 3 hours
Insurers and regulatory agencies expect regular internal controls and documented self-inspections. In this concise training course, participants learn how to systematically identify, document, and assess risks.

Contents

- Fundamentals of insurance-related internal controls
- Conducting structured facility inspections
- Identifying typical vulnerabilities
- Fire safety and security inspections
- Documentation and record-keeping
- Preparing for insurance and regulatory audits

Benefits

- Early detection of risks
- Greater audit and insurance compliance
- Standardized and traceable inspections
- Improved safety culture

Certificate

- Proof of participation and competence
- IDD points

Cyber Security & NIS2

Online Training | approx. 3 hours

Cyber incidents are among the fastest-growing risks for industrial companies. This training covers the fundamentals of cyber risks, as well as the requirements of the NIS2 Directive and its implications for businesses.

Contents

- Fundamentals of Information Security
- Current Cyber Threats
- NIS2 Requirements
- Roles and Responsibilities
- Emergency Response and Reporting Obligations

- Protection of critical business processes
- Cyber resilience and BCM

Benefits

- Understanding of regulatory requirements
- Reduction of cyber risks
- Preparation for NIS2 compliance
- Improved crisis management and response capabilities

Certificate

- Proof of participation and competence
- IDD points

Risk Protection Officer (RPO)

Certification Course | 32 hours | In-Person

The Risk Protection Officer course is the core training program for anyone who wants to actively manage and assess risks in industrial companies. The course combines risk management, fire safety, business interruption, natural hazards, cyber risks, and insurance requirements into a holistic approach..

Contents

- Industrial Risks and Causes of Damage
- Risk Analysis and Risk Assessment
- Fire Safety and Explosion Protection
- Insurance Requirements and Audits
- Natural Hazard Management
- Business Continuity Management
- Business Interruption Risks
- Self-Inspections and Audits
- Management of Change
- Practical Site Inspections

Benefits

- Comprehensive understanding of risk
- Increased organizational resilience
- Preparation for insurance and regulatory requirements
- International best practices
- Certified proof of competence

Certificates:

- Fire Safety Officer, Austria (TRVB 117 O)
- Fire Safety Officer, Germany (depending on the partner organization and training program)
- Certificates of attendance and competence
- IDD points

Methods and standards

Our consulting services are based on recognized international and national standards, proven methods, and actuarial best practices. For us, these standards are not an end in themselves, but rather serve as a structured foundation for assessing risks in a transparent manner, prioritizing measures based on cost-effectiveness, preparing documentation in a manner that stands up to audit scrutiny, and providing sound justification for decisions to management, insurers, regulatory authorities, auditors, and stakeholders. Depending on the task at hand, we combine management system standards, technical regulations, insurance standards, and regulatory requirements into a practical consulting approach that is both technically sound and implementable in day-to-day operations.

ISO 31000 – Risk management

ISO 31000 is the internationally recognized guideline for structured, integrated, and continuous risk management. The standard describes principles, a framework, and a process for identifying, analyzing, evaluating, treating, monitoring, and communicating risks. risk on mind uses ISO 31000 as a methodological foundation to assess risks not in isolation, but in the context of corporate objectives, strategy, processes, investments, and insurability. This results in transparent decision-making frameworks that integrate technical, organizational, and economic aspects.

Benefits for our customers

- **Greater transparency regarding business risks:**
  Risks are systematically identified, assessed, and documented. This fosters a shared understanding of which risks are material and what impact they may have on corporate objectives.
- **Improved management decisions:**
  Decisions are based on transparent assessments, clear criteria, and reliable risk information rather than on individual opinions or gut feelings.
- **Reduction of uncertainties:**
  Through structured analysis, assessment, and monitoring, uncertainties become visible and manageable. Companies can consciously avoid, reduce, transfer, or accept risks.
- **Economically optimized risk management:**
  Measures are prioritized based on risk, impact, feasibility, and cost-benefit ratio. As a result, investments are targeted where they make the greatest contribution to risk reduction.

ISO 22301 – Business Continuity Management

ISO 22301 defines the requirements for a Business Continuity Management System and helps organizations maintain or quickly restore critical business processes even in the event of disruptions, crises, or incidents. The standard integrates business impact analysis, risk analysis, recovery strategies, emergency planning, exercises, tests, and continuous improvement into a structured management system. risk on mind uses ISO 22301 to identify business interruption risks and develop practical continuity strategies for critical processes, locations, supply chains, IT systems, and resources.

Benefits for our customers

- **Reduced business interruptions:**
  Critical processes and dependencies are identified, assessed, and safeguarded with appropriate protection and recovery measures.

- **Faster recovery of critical processes:**
  Recovery strategies, responsibilities, communication channels, and resources are defined in advance. This enables a faster and more coordinated response in the event of an incident.
- **Greater resilience and crisis resistance:**
  Organizations are better prepared to respond in a structured manner to cyber incidents, natural disasters, supply chain disruptions, technical failures, or other crises.
- **Verifiable continuity planning:**
  BCM documentation, exercises, tests, and management reviews provide robust evidence for customers, insurers, auditors, regulatory authorities, and owners.

ISO 27001 – Information security

ISO/IEC 27001 is the globally recognized standard for information security management systems. It helps organizations systematically identify, assess, and address risks to the confidentiality, integrity, and availability of information. The standard establishes a framework for information security policies, risk treatment, controls, responsibilities, internal audits, and continuous improvement. risk on mind integrates ISO 27001 with NIS2, BCM, cyber resilience, and operational risk management so that information security is understood not only as a technical matter but also as a management and governance responsibility.

Nutzen für unsere Kunden

- **Reduzierung von Cyber- und Informationssicherheitsrisiken:**
  Risiken für Daten, Systeme, Prozesse und Informationen werden strukturiert bewertet und mit geeigneten organisatorischen, technischen und physischen Maßnahmen behandelt.
- **Schutz sensibler Informationen:**
  Vertraulichkeit, Integrität und Verfügbarkeit relevanter Informationen werden durch klare Verantwortlichkeiten, Zugriffsregelungen, Sicherheitsprozesse und Kontrollmechanismen gestärkt.
- **Verbesserte Compliance:**
  ISO 27001 unterstützt die Erfüllung gesetzlicher, vertraglicher und regulatorischer Anforderungen und bildet eine starke Grundlage für NIS2-Readiness, Kundenaudits und Zertifizierungen.
- **Höheres Vertrauen von Kunden und Geschäftspartnern:**
  Ein nachvollziehbares Informationssicherheits-Managementsystem zeigt, dass Sicherheitsrisiken aktiv gesteuert werden und sensible Informationen professionell geschützt sind.

NIS2

Die NIS2-Richtlinie erweitert die europäischen Anforderungen an Cybersecurity, Governance und Resilienz für wesentliche und wichtige Einrichtungen. Sie fordert ein risikobasiertes Sicherheitsmanagement, klare Verantwortlichkeiten der Leitung, Maßnahmen zur Prävention und Reaktion auf Sicherheitsvorfälle, Lieferkettensicherheit, Meldeprozesse, Business Continuity und nachweisbare Schutzmaßnahmen. risk on mind unterstützt Unternehmen dabei, NIS2 nicht als isoliertes IT-Projekt umzusetzen, sondern mit ISO 27001, BCM, Risikomanagement, Dienstleistersteuerung und Versicherbarkeit zu verbinden.

Benefits for our customers

- **Compliance with regulatory requirements:**
  Companies gain clarity on which NIS2 requirements are relevant, what gaps exist, and which measures must be implemented as a priority.
- **Reduced cyber and operational risks:**

Cyber risks are assessed in conjunction with operational dependencies, critical processes, service providers, and recovery requirements.

- **Improved crisis resilience:**
  Incident response processes, reporting channels, escalation procedures, crisis management structures, and recovery measures are established and regularly reviewed.
- **Greater insurability in the cyber domain:**
  Transparent security measures, documentation, and governance strengthen the organization's position with cyber insurers and improve transparency in insurance processes.

CER – Critical Entities Resilience Directive

The CER Directive aims to strengthen the resilience of critical infrastructure against physical, technical, organizational, and natural hazards. At its core is an all-hazards approach that considers critical services, locations, infrastructure, supply chains, personnel dependencies, protective measures, emergency response organization, and recovery capabilities as a unified whole. risk on mind leverages the CER requirements to integrate regulatory resilience with risk management, BCM, security concepts, documentation, and customer training.

Benefits for our customers

- **Greater operational resilience:**
  Critical services, locations, and dependencies are identified and safeguarded through appropriate organizational, technical, and structural measures.
- **Systematic assessment of all sources of risk:**
  Natural hazards, technical failures, cyber incidents, physical threats, supply chain issues, and organizational vulnerabilities are evaluated collectively.
- **Improved emergency preparedness:**
  Emergency plans, recovery strategies, communication channels, drills, and responsibilities are clearly defined and regularly reviewed.
- **Future-proof compliance:**
  Companies can meet regulatory requirements in a structured manner and demonstrate their resilience to authorities, customers, insurers, and stakeholders in a transparent way..

COSO Enterprise Risk Management (ERM)

COSO Enterprise Risk Management integrates risk management with strategy, performance, governance, and corporate management. Risks are viewed not only as threats, but also as factors that influence the achievement of objectives, value creation, the quality of decision-making, and corporate development. risk on mind applies COSO ERM particularly in situations where risk management needs to be more closely linked to management decisions, shareholder interests, governance structures, and strategic management.

Benefits for our clients

- **Better strategic decisions:**
  Risks are considered in the context of corporate objectives, strategy, performance, and value creation.
- **Linking risk to corporate objectives:**
  Management and owners recognize which risks significantly influence the achievement of objectives and which measures are strategically relevant.
- **Greater corporate controllability:**
  Risk information is integrated into reporting, planning, investment decisions, and governance processes.
- **Sustainable value enhancement:**

Risks are not only reduced but actively managed to stabilize, safeguard, and further develop corporate value.

FM Global Data Sheets

- FM Global Data Sheets are among the world's most important technical guidelines for industrial loss prevention and insurability. They are based on extensive loss analysis, research, and underwriting experience and contain detailed recommendations on fire protection, storage, sprinkler systems, natural hazards, building protection, maintenance, and operational risks. risk on mind utilizes FM Global Data Sheets in particular for international industrial companies, complex production sites, and insurance-related protection concepts.

Benefits for Our Clients

- **Improved insurability:**
  Protective measures are aligned with internationally recognized underwriting requirements, making them more transparent to insurers.
- **Optimized protection concepts:**
  Technical protective measures are developed in a practical, risk-based manner and tailored to the specific site.
- **Reduction of property damage and business interruption losses:**
  Loss prevention, fire containment, natural hazard protection, and technical redundancies reduce the likelihood and impact of major losses.
- **Recognition by international insurers:**
  Alignment with FM Global Data Sheets facilitates communication with international industrial insurers and reinsurers.

NFPA (National Fire Protection Association)

The NFPA standards of the National Fire Protection Association are internationally recognized codes and standards for fire protection, fire suppression systems, electrical safety, hazardous materials, industrial protection systems, and organizational safety measures. They are used in particular for international projects, global insurance programs, technical protection concepts, and industrial facilities with high fire or explosion risks. risk on mind uses NFPA requirements to ensure that technical protective measures are internationally comparable, insurable, and audit-ready.

Benefits for clients

- **Internationally recognized safety standards:**
  NFPA requirements provide a robust technical foundation for international locations, insurance programs, and audits.
- **Reduced fire damage:**
  Clear requirements for fire suppression systems, early fire detection, electrical safety, and organizational measures effectively reduce fire risks.
- **Improved safety of facilities and infrastructure:**
  Technical systems, buildings, production areas, and critical infrastructure are assessed according to recognized safety principles.
- **Greater acceptance by insurers:**
  Alignment with NFPA standards facilitates coordination with international insurers and technical risk engineers.

VdS Guidelines

The VdS guidelines are among the most important European standards for loss prevention, fire protection, burglary protection, fire suppression systems, security organization, and insurance requirements. They are used by many insurers as a technical reference and help companies implement protective measures in a way that is transparent, verifiable, and insurable. risk on mind primarily uses VdS guidelines when evaluating and optimizing security systems, fire protection organizations, and insurance-related measures.

Benefits for our clients

- **Improved insurance terms:**
  Transparent security measures based on VdS principles can strengthen your negotiating position with insurers.
- **Demonstration of high security standards:**
  Technical and organizational protective measures are documented based on recognized guidelines and made verifiable.
- **Reduced likelihood of damage:**
  Clear requirements for prevention, detection, alarm, and suppression make it more likely that damage events will be prevented or limited.
- **Clear technical guidance:**
  Companies receive a structured foundation for the planning, operation, maintenance, and improvement of protection systems.

European Standards

European standards (EN standards) define uniform technical, organizational, and safety-related requirements for products, systems, processes, and services within Europe. They form the basis for the harmonized planning, construction, testing, operation, and maintenance of technical systems and are regularly referenced by regulatory authorities, insurers, experts, planners, operators, and manufacturers. risk on mind uses the relevant EN standards to evaluate technical systems, buildings, processes, and organizational measures in terms of safety, availability, reliability, compliance, and insurability.

Benefits for our clients

- **Enhanced Safety**
  Technical systems and organizational processes are evaluated and optimized based on recognized European standards.
- **Demonstrable Compliance**
  Compliance with relevant standards supports demonstration of compliance to authorities, customers, certification bodies, and insurers.
- **Risk reduction**
  Potential vulnerabilities are identified early, and targeted measures to minimize risk are developed.
- **Higher system availability**
  Standard-compliant planning, testing, and maintenance improve operational safety and reduce unplanned outages.
- **Protection of People, Property, and the Environment**
  The application of established technical standards helps prevent or limit damage and operational disruptions.
- **Improved Insurability**
  Adherence to recognized European standards increases transparency and acceptance among insurers, risk engineers, and financial institutions.
- **Future-Proof Investments**
  Companies create a robust foundation for sustainable investment decisions and future regulatory requirements.

- **Uniform basis for evaluation**
  The application of harmonized standards makes technical evaluations, audits, and risk analyses traceable and comparable

TRVB – Technical Guidelines for Preventive Fire Protection

In Austria, the Technical Guidelines for Preventive Fire Protection specify essential requirements for fire protection organization, self-inspections, fire alarm systems, fire suppression systems, escape routes, workplace fire protection, and structural and technical fire protection measures. In many areas, they represent the recognized state of the art and are of great practical importance to operators, fire safety officers, authorities, insurers, and experts. risk on mind uses TRVB guidelines to implement Austrian requirements in a legally compliant, practical, and insurance-relevant manner.

Benefits for our clients

- **Legal certainty:**
  Fire safety measures are aligned with recognized Austrian guidelines and are thus justified in a transparent manner.
- **Practical implementation of Austrian requirements:**
  TRVB specifications are translated into operational processes, self-inspections, documentation, and fire safety organization.
- **Enhanced protection of people and property:**
  Preventive measures, organizational structures, and technical protection systems reduce fire risks and improve safety in the workplace.
- **Optimized fire safety organization:**
  Roles, responsibilities, training, inspections, and monitoring obligations are clearly defined and permanently embedded within the company.

OIB-Guidelines

In Austria, the OIB Guidelines define fundamental structural engineering requirements for buildings, particularly in the areas of fire protection, safety of use, accessibility, hygiene, health, environmental protection, sound insulation, and energy conservation. For industrial and commercial projects, they serve as an essential foundation for planning, permitting, implementation, and operator responsibility. risk on mind uses OIB guidelines to align building code requirements with fire safety, risk mitigation, insurability, and cost-effective project implementation.

Benefits for our clients

- **Legally compliant project implementation:**
  Building code requirements are addressed early on and integrated into planning, permitting, and implementation.
- **Reduction of planning and permitting risks:**
  Conflicts between project planning, regulatory requirements, fire safety, and insurability are identified and mitigated early on.
- **Compliance with regulatory requirements:**
  OIB guidelines provide a clear basis for coordination with authorities, planners, experts, and project stakeholders.
- **Operational and investment security:**
  Legally compliant and risk-based planning supports long-term operational reliability, lower retrofitting costs, and better investment decisions.

Certificates and Qualifications

IDD-certified continuing education

Accredited training provider for the continuing education of insurance brokers and insurance agents, offering IDD-eligible hours.

Seal of quality

Continuing Education for Insurance Brokers and Insurance Advisors

The risk on mind Academy has been awarded the corresponding seal of quality as a continuing education provider.

Continuing Education for insurance agents

Recognized continuing education institution for insurance agents.

Certified Business Continuity Manager (CBCM)

Martin Lanznaster's training and certification as a Certified Business Continuity Manager are documented.

BSB-Weiterbildungszertifikat Österreich (TRVB 117 O)

The RPO training program is conducted in collaboration with a recognized training institute and includes the continuing education certificate for fire safety officers in accordance with TRVB 117 O.

Added value for our customers

Our services lay the foundation for better decisions, greater resilience, and sustainable business success. Tangible added value is created when risks are not only identified but also actively managed, economically assessed, and permanently embedded within the organization. risk on mind combines consulting, data, digital solutions, standards, and training into an integrated approach that makes companies more resilient, better equipped to make decisions, and more successful in the long term.

A key factor in this success is the training of the company's own employees. Risks arise and evolve in day-to-day operations—in production, logistics, maintenance, IT, procurement, facility management, compliance, fire safety, management, and at company locations. When internal teams can identify risks early on, conduct internal controls, track measures, maintain documentation, and respond appropriately in the event of an incident, risk management becomes a genuine capability of the company. This reduces dependence on individual external measures, increases the speed of implementation, and strengthens the risk culture.

The added value, therefore, lies not only in reports, analyses, or concepts, but in the company's long-term capacity to act. Knowledge translates into the ability to act; the ability to act fosters resilience; and resilience leads to economic strength. Companies can better manage risks, prioritize investments more effectively, improve their insurability, pass audits with greater confidence, and maintain their ability to act even in crisis situations.

Your added value at a glance

- **Greater Resilience:**
  Companies remain capable of operating even in the face of crises, operational disruptions, cyberattacks, natural disasters, or supply chain disruptions. Critical processes are better protected, recovery times are shortened, and decisions are made more quickly when incidents occur.
- **Lower loss costs:**
  Through early risk identification, effective protective measures, and clear lines of responsibility, losses can be prevented or their impact significantly reduced. This lowers not only direct loss costs but also consequential costs resulting from downtime, contractual penalties, delivery delays, or reputational damage.
- **Improved insurability:**
  Transparent risk exposures, reliable data, traceable protection concepts, and documented measures increase a company's appeal to insurers. Companies can better negotiate requirements, demonstrate risk improvements, and support stable, long-term insurance solutions.
- **Reduced downtime:**
  Critical processes, equipment, IT/OT systems, supply chains, and infrastructure are specifically analyzed and secured. This helps limit business interruptions, improve recovery strategies, and reduce the economic impact of disruptions.
- **Greater Compliance:**
  Regulatory requirements such as NIS2, CER, CSRD, ISO 27001, or ISO 22301 are not addressed in isolation but are efficiently integrated into existing management, risk, and compliance processes. This reduces bureaucracy, enhances traceability, and strengthens security during audits
- **Better Management Decisions:**
- Objective risk analyses, statistical data, economic assessments, and clear priorities create a robust foundation for investments, action planning, risk transfer, and strategic decisions. Management and owners can identify which measures actually create value.

- **Training in-house staff as a sustainable value contribution:**
  Targeted training of internal teams strengthens the company from within. Employees can identify risks in day-to-day operations, conduct internal controls, document deviations, track measures, prepare for audits, and respond in a structured manner in the event of an incident. This builds risk competence within the company on a lasting basis.
- **Reduced dependence on individual external measures:**
  When employees can independently take on key tasks, processes become faster, more efficient, and more robust. External consulting remains important for methodology, quality assurance, and further development, but the company gains its own capacity for action and operational strength.
- **A stronger risk culture and clear lines of responsibility:**
  Trained employees have a better understanding of risks and take responsibility for managing them. As a result, controls, measures, and improvements are not only documented but also put into practice on a daily basis. This strengthens safety awareness, personal responsibility, and collaboration between departments.
- **Faster implementation and higher-quality measures:**
  In-house expertise accelerates the implementation of protective measures, compliance requirements, and improvement programs. Measures are better understood, planned more realistically, pursued more consistently, and implemented more sustainably.
- **Protection of reputation and corporate value:**
  Reliable processes, high security, demonstrable risk management, and trained employees strengthen the trust of customers, employees, investors, insurers, regulatory authorities, and business partners. This protects reputation, delivery capability, and corporate value in the long term.
- **Sustainable integration into the organization:**
  The greatest added value is created when risk management, BCM, compliance, ESG, information security, and risk protection are viewed not as individual projects but as enduring capabilities of the organization. Consulting, software, standards, and training are interlinked and make the organization more resilient and economically stronger in the long term..

Our goal

We help companies turn risks into a competitive advantage.

Whether it's risk management, business continuity management, insurance engineering, cybersecurity, compliance, ESG, risk protection strategies, rismo®, or the Academy—each of our services pursues the same goal: risks should not only be managed but also translated into measurable corporate value.Schäden vermeiden und deren Auswirkungen reduzieren

- Prevent losses and reduce their impact
- Protect corporate value, earnings, and reputation
- Improve insurability and risk transfer
- Increase resilience and operational capacity
- Strengthen management decisions with robust data
- Train internal employees and empower them to manage risks independently
- Permanently embed risk competence within the company
- Ensure future viability, competitiveness, and economic strength

After all, risk management is not an end in itself. It is intended to make companies more successful, more resilient, and economically stronger—and to empower their own employees to recognize, properly assess, and effectively manage risks in their day-to-day work.

Contact

risk on mind® GmbH

office@riskonmind.eu

+43 (1) 343 03 09

Headquarter Wien:

Postgasse 16/21
1010 Vienna
Austria

Office Österreich:

Prinz Eugenstraße 45/8
2301 Groß-Enzersdorf
Austria

www.riskonmind.eu

LinkedIN: @riskonmind