RISK MANAGEMENT · belongs at · C-LEVEL

The End of *3-Year Strategic Planning.*

The world is changing faster than any strategic plan. There is one leadership tool that keeps pace – and that the EU already mandates.

ISO

31000

International Standard for Risk Management

WHAT IS ISO 31000?

Not Bureaucracy.
A Thinking Framework for Leadership.

01 **Principles**

Risk and Opportunity as Value Creation

Understanding risk as a strategic variable – not as a threat to be avoided.

02 **Framework**

Anchored at Leadership Level

Clear accountabilities, resources, and communication at C-Level.

03 **Process**

Continuous Cycle

Identify, Assess, Treat, Monitor, Communicate – continuously.

5 Steps. Continuous. Not a one-time event.

The process is not a project – it is a leadership routine.

01

Define Context

Precisely define internal & external factors, stakeholders, and objectives

02

Identify Risks

What could happen? Where, why, and with what consequences?

03

Assess Risks

Likelihood × Impact = Prioritization

04

Treat Risks

Avoid, reduce, transfer, or consciously accept

05 Monitor & Communicate — Continuous monitoring & reporting at leadership level

EU REGULATION

5 Laws.

1 Common Core.

NIS2

Cyber risk management as a legal duty. Personal CEO liability. Applies from 50 employees or €10M revenue.

DORA

ICT risk management in the financial sector. Fines up to 2% of global annual turnover.

AI Act

Mandatory risk classification for AI systems. Penalties up to €35M or 7% of turnover.

CRA

Cyber Resilience Act: Security by Design – risk management across the entire product lifecycle.

DSGVO

Data Protection Impact Assessment (DPIA) as a formalized risk instrument. Article 32 GDPR.

Source: NIS2UmsuCG, DORA, EU AI Act, CRA, GDPR

Why Risk Management Outperforms Controlling & Strategic Plans.

Yesterday

— 3-Year Plan: rigid, often outdated within 6 months

— Controlling: looks in the rear-view mirror

— Reactive: damage only becomes visible after it occurs

— Decisions based on historical data

— Risk as a disruptive factor – not as a variable

Today: ISO 31000

✓ Rolling & dynamic – adapts to reality

✓ Forward-looking: scenarios & early warning signals

✓ Proactive: risks addressed before they cause damage

✓ Real-time decisions with risk clarity

✓ Risk as a strategic management variable

C-LEVEL RESPONSIBILITY

Risk Management is The CEO's Business. Not IT's.

⚖ Personal Liability

NIS2 & DORA explicitly assign responsibility to the CEO. No delegation possible – with real consequences.

◎ Strategic Decision Basis

Every investment, every partnership, every product – decided with risk clarity, not gut feeling.

▲ Measurable Competitive Advantage

Customers, partners, and investors prefer companies with robust, demonstrable risk management.

◈ Resilience in Times of Change

AI super-cycle, cyber threats, regulatory waves – only those who know their risks navigate change with confidence.

CONCLUSION

Risk Management is not a burden.
It is your license to grow.

Those who embed risk management as a strategic leadership tool simultaneously fulfills NIS2, DORA, AI Act, CRA, and GDPR – and makes faster, safer, and more confident decisions than the competition.

Have you already embedded risk management at C-Level – or are you still fighting with isolated measures and annual plans?

We support companies in establishing risk management for what it truly is: the operational backbone of modern leadership. Let's talk.

#RiskManagement #ISO31000 #NIS2 #DORA #CyberSecurity #Compliance #CLevel #AIAct #SME