t2p solutions oü
bringing trains2people

KRITIS ~ NIS

Wie man Risiko Management in einen Unternehmensvorteil verwandeln kann

How to turn Risk Management into a benefit

www.t2psolutions.com
info@t2psolutions.com
Katusepapi 4/2, 11412 Tallinn (Estonia)

speaker

Lars Zimmermann, Executive Board Member

- Head of Strategy & Business Development
- University of Gießen: Masters in Business Administration: Transportation Econ. & Informatics
- Pilot on Boeing 757/767 & Airbus A321neo
- Compliance & Safety Risk Manager/ Lead Auditor
- International Consultant and Project Manager
- Member of the German Association of Transportation Science (DVWG e.V.)
- Dangerous/ Hazardous Goods Expert & Instructor
- Communication & Human Performance Instructor
- Crisis Management Team of Lahn-Dill-Kreis /Region
- Speaker & Author

Lars Zimmermann
Born 1974
Wetzlar (D)
Riga (LV)
Tallinn (EE)

Overview

compliance

software: Human Factor

the systematic approach

hardware: technology

the smarter way: better decisions – better outcomes

Stephen Hawking

„Success in creating AI would be the biggest event in history. Unfortunately, it might also be the last, unless we learn how to avoid risks.“

Leverhulme Centre for the Future of Intelligence (LCFI) at Cambridge University in 2016

Current status – compliance aspects – hard law

- Basis: Cybersecurity Act Regulation (EU) 2019/881 (ENISA)
- EU AI Act Regulation 2024/1689; in force since 01.08.2024: Annex III Hochrisikosystem KI (KI in z.B. OPS Systemen der kritischen Infrastruktur & Sicherheitssystembauteilen) tritt am **02.08.2026** in Kraft
- EU Directive / Richtlinie (EU) 2022/2555 (NIS2-Richtlinie)
- Germany: „NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG), das das BSI-Gesetz grundlegend reformiert (BSIG-neu). Zentrale Paragraphen sind **§28 (Betroffenheit – ÖPNV KRITIS), §30 (Risikomanagement), §32 (Meldepflichten)**, §38 (Geschäftsleitungspflichten) und §65 (Bußgelder)“
- Since 06.12.2025 in force (no transition period)
- Registration due date: 06.03.2026 -> Extended to: **31.07.2026**
- Personal liability of directors!!! Accountability
- Penalties

Why KRITIS and why it is more important than ever?

- Zunehmende Abhängigkeit von vernetzten Systemen
- Steigende Bedrohungslage (Cyber, Energie, Personal, Lieferketten)
- Höhere regulatorische Anforderungen (KRITIS-Dachgesetz, NIS2, EU-Resilience-Standards)
- Erwartungshaltung von Politik, Öffentlichkeit und Nutzern
- Notwendigkeit, Projekte und Budgets planbar zu halten

Kernaussage:
KRITIS ist kein Compliance-Thema – es ist ein Führungs- & Steuerungsinstrument.

Organisations need a common framework that connects risk management directly to objectives, decisions and delivery. Without that consistency, different teams inevitably develop different approaches.

Cybersecurity & Risk Mgmt. not only as a matter of MUST

- EU Regulation No 402/2013 on the CSM (common safety method) for risk evaluation and assessment for RUs & IMs
- An active Risk Management to …
    - ✓ Guarantee safe & secure operations
    - ✓ Identify and mitigate Risks
    - ✓ Remain situational awareness (decission making)
    - ✓ Manage shared risks acroos different stakeholders
    - ✓ Unleash efficiency potentials & meet project times as well as budgets

§30 Risik Management measures (BSI-Gesetz)

- (1) … verpflichtet, geeignete, verhältnismäßige & wirksame technische u. organisatorische Maßnahmen … zu ergreifen
- … um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse … zu vermeiden … Auswirkungen möglichst gering halten (Fall-Back-Solutions)
- Dokumentation, Auditierungs- & Meldeverpflichtung

Do not forget: an integrated, comprehensive & Reporting- / Feedbacksystem!

§30 Risik Management measures (BSI-Gesetz)

(2) Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten, … und müssen auf einem gefahrenübergreifenden Ansatz beruhen. Die Maßnahmen müssen zumindest Folgendes umfassen:

1. Konzepte … **Risikoanalyse** und auf die Sicherheit in der IT
2. Bewältigung von Sicherheitsvorfällen,
3. Aufrechterhaltung des Betriebs, … W**iederherstellung nach einem Notfall, und Krisenmanagement**,
4. **Sicherheit der Lieferkette** einschließlich sicherheitsbezogener Aspekte der Beziehungen …
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von IT-Systemen, Komponenten und **Prozessen**, einschließlich Mgmt. und **Offenlegung von Schwachstellen**,
6. …**Bewertung der Wirksamkeit von Risikomanagementmaßnahmen** im Bereich der Sicherheit in der Informationstechnik,
7. **grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der IT-Sicherheit**
8. Konzepte und Prozesse für den Einsatz von kryptographischen Verfahren,
9. … **Konzepten für die Sicherheit des Personals**, die Zugriffskontrolle und für die Verwaltung von IKT-Systemen, -Produkten und -Prozessen,
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung … ggf. gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung

§32 Reporting requirements (BSI-Gesetz) to BSI

Phase 1: **immediately**, max. within 24h	->	unlawful, malicious crossborder impact?
Phase 2: **within 72h**	->	threat confirmed? 1st estimation of severity & impact **Indicators of compromise**
Phase 3: potentially	->	BSI request on updates
Phase 4: **1 month**	->	Final report (comprehensive analysis, type & source intrution, counter measures, cross-border impact)

Phase 5: Final report, when finished (if intrution was still ongoing after 1 month)

Why HOF? +++ Human Organisational Factors

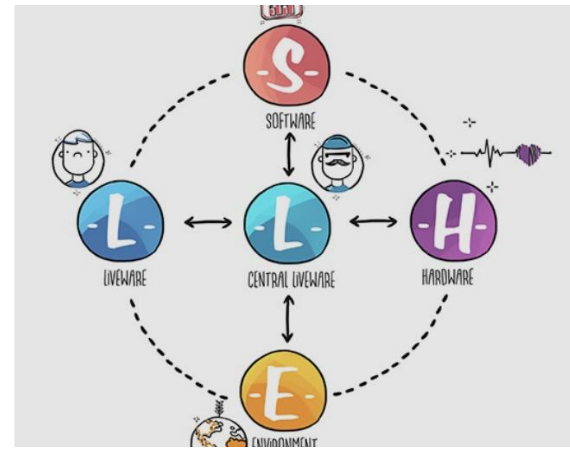
- NASA and various aviation companies' workshop 1979 is regarded as the origin of this **training & communication approach** (KLM TFN 1977 & United UA173 1978).
- Humans, as part of **organisational structures,** are the cause of a large number of accidents (aviation and other sectors (mandatory in the rail sector: Directive EU 798/2016)
- Human Factors training go hand in hand with the requirement for SMS **(safety management system)** for infrastructure managers & railway undertakings.

Famous quotes – understanding the logic

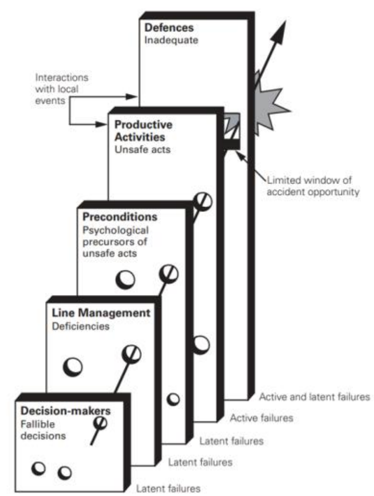
"Unrealized potential is one of the greatest pains there is. Don't live with it.“
It serves as a powerful **call to action** to lean into your **goals, tackle your fears**, and pursue **continuous growth (improvement)**. Scott Hamilton (Olympique Goldmedal Winner Skating 1984)

Human – Organisation – Technology – External Factors

- Human Error: It‘s a complex world
- Root cause: organisational setup
- Risk identification is key
- Reporting & Communication culture
- Situational Awareness (information / data availibilty)
- Decision making



70-80% of human error lead to accidents or incidents across industries!
Chalmers University of Technology Sweden



Benefits of human centric approach

€ **ident**: of risks & threats across all processes / supply chains

€ **reduce**: the number of accidents/ incidents (and therefore the subsequent costs: operation interruptions, loss of experienced team members, damage claims, loss of reputation, etc.).

€ **encourage**: learn and practice safety, but also to improve processes and thus increase their efficiency

€ employee **participation** = identification with the company

€ enabler for new technology, **innovation & customer satisfaction**

worth a thought…

"the safest companies are also the most efficient"

International Civil Aviation Organization

worth a thought...

Problem Statement

RISK WELL

- Unprecedented change is the norm
- Current risk and project management tools aren't delivering the right outcomes
- Cost overruns, delays and poor outcomes are normal

37% **of capital projects overrun by 20%+ due to poor risk management**
(KPMG)

99.5% **of big projects miss time, budget, or benefits**
(Harvard Business Review)

28% **of project failures directly caused by weak risk management**
(Econstor)

Typical business areas and their risks

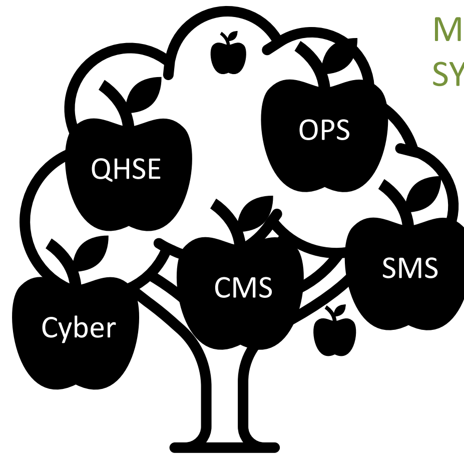
Strategy –Resilience – Processes – Ressources

Example checks:

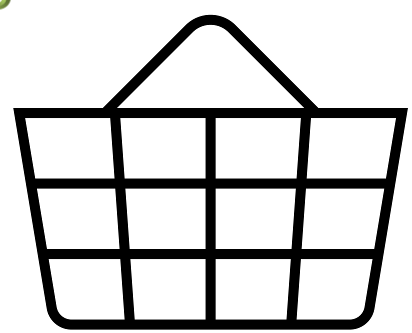
all (critical) process idetfified?
are there redundencies?
are ERP up-to-date & trained?
supply chains secured?
IT-Systems KRITIS-conformity?
are roles and responisbilites defined & clear to everybody?
defined communication in a crisis?

systematic approach

Strategy –Resilience – Risk Management



RESOURCES



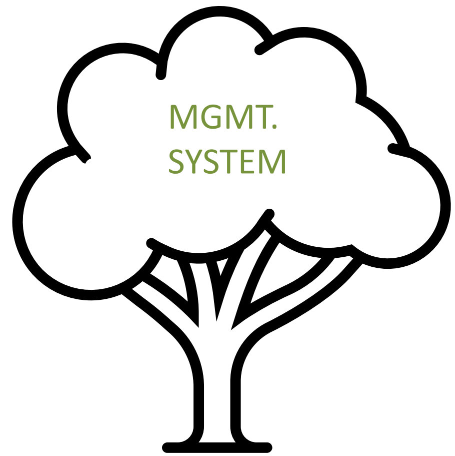
RISK MANAGEMENT

Why Traditional Risk Management Often Falls Short

The Common Pattern

✓ Risks identified
✓ Risks logged
✓ Risks reported
✗ Decisions unchanged
✗ Priorities unchanged
✗ Resources unchanged

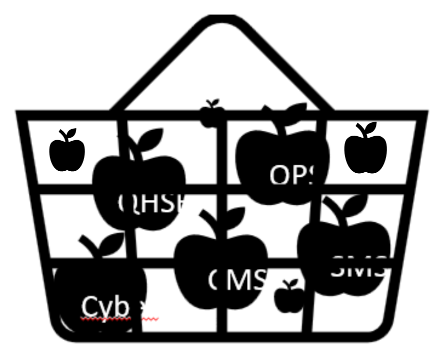
Decision	Uncertainty
Fleet replacement	Supplier performance
Signalling upgrade	Technology integration
New station delivery	Planning approvals
Timetable changes	Passenger demand
Maintenance strategy	Asset reliability



Result

- The risk register exists.
- The outcome remains unchanged.

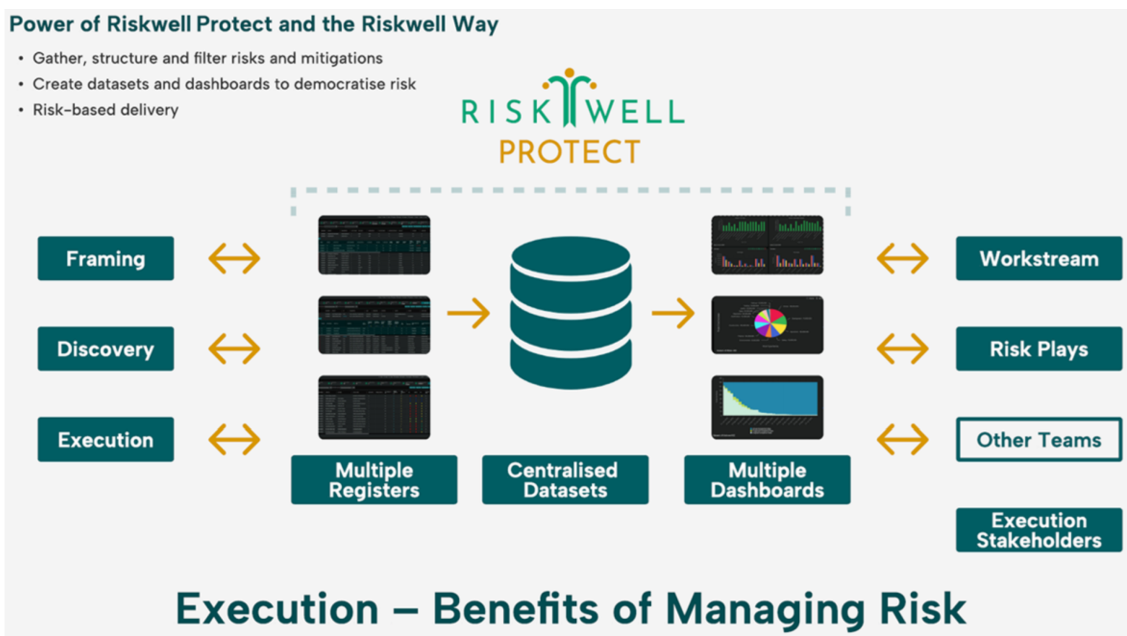
Risk → Decisions → Delivery → Outcomes



DELIVERY
RISK MANAGEMENT

How to unleash your organisational potentials?
(e.g. Riskwell Protect)

- Implement a wholistic Delivery Risk Management:
  Organisations need a common framework that **connects risk management directly to objectives, decisions and delivery**. Without that consistency, different teams inevitably develop different approaches.

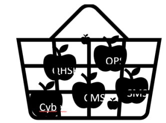


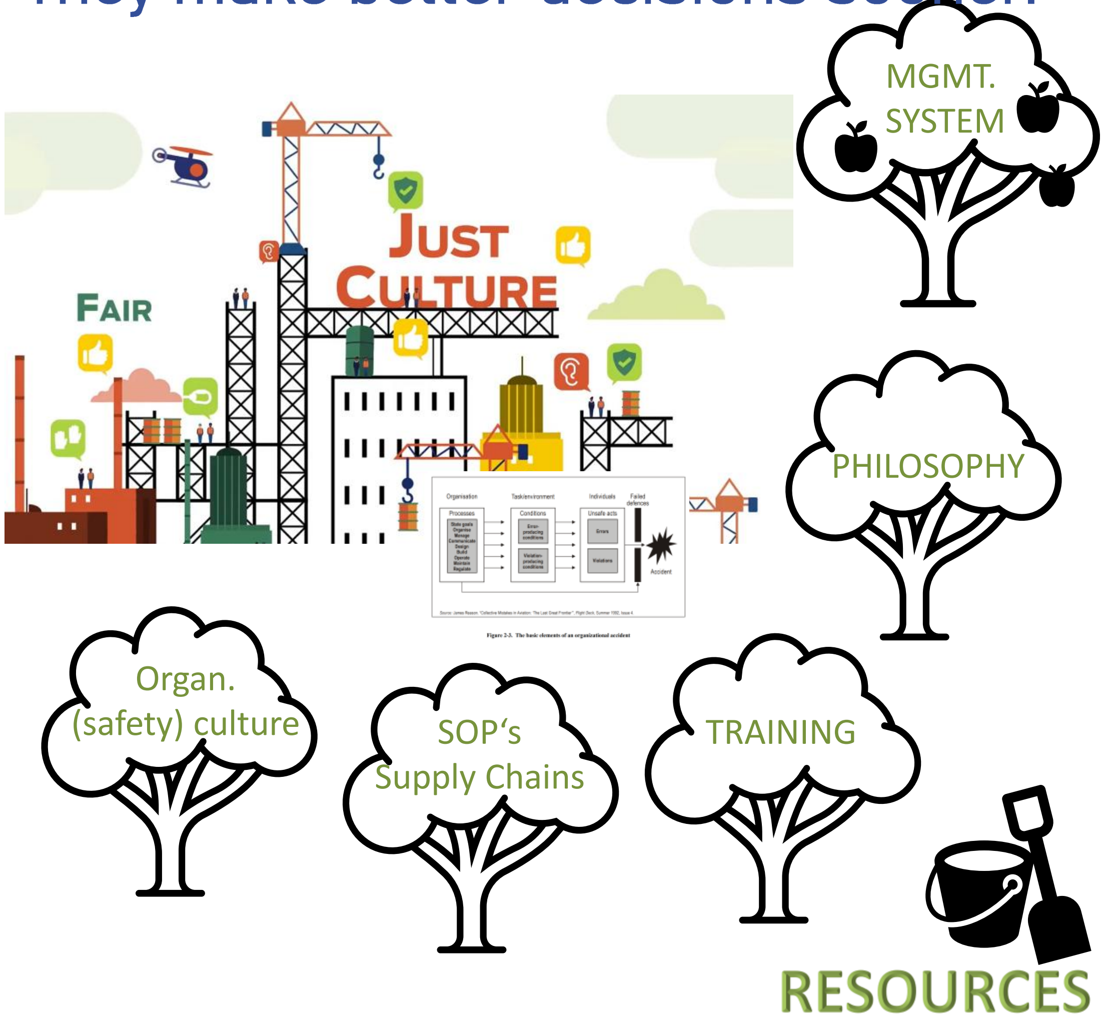
How to unleash your organisational potentials

- Implement a Strategy & Organisational Philosophy (especially also for the use of AI)
- Training, Training, Training: Awareness raising & Investment into human capital
- SMS/ CMS to identify more than safety risks
  (Note: **Financial risks will transform into (Safety) Threats one day!**)
- Incl. all stakeholders & employees – everybody is responsible to ident, manage and mitigate risks as well as identifying opportunities (potentials)

summary: smarter way

The best organisations don't manage risks better. They make better decisions sooner.





✓ Earlier identification of uncertainty
✓ Better prioritisation of limited resources
✓ More informed investment decisions
✓ Improved project and operational performance
✓ Greater resilience
✓ Stronger public accountability
✓ Better protection of public investment
✓ More reliable public services

Bring partners & expertise on board

THE CYBER EAGLE PROJECT INC.

RISKWELL

The Riskwell and t2p Partnership

Powering successful delivery of projects, initiatives and strategy

t2p trains2people solutions

THE RISKWELL + T2P PARTNERSHIP

Expertise. Methodology. Technology. Training. Outcomes.

A unique combination of deep delivery and risk expertise, proven methodology, market-leading technology and people capability development.

Together, we help organisations embed risk at the heart of delivery to achieve better decisions, stronger performance and outstanding outcomes.

RISKWELL PROTECT

The delivery-focused risk management system – built for outcomes, not just tracking risks.

Purpose-built for delivery, not generic risk management.

Links risk to business outcomes, impact and value.

Real-time insight for confident, evidence-based decisions.

Designed to drive accountability, transparency and risk ownership across teams.

Enables proactive management that keeps delivery on track and outcomes in sight.

RISKWELL WAY

The risk-led delivery methodology that turns uncertainty into confidence and strategy into results.

Uses risk as the primary driver for planning, prioritisation and delivery.

Focuses on what matters most – outcomes, value and strategic intent.

Adapts to complexity and change without compromising control.

Builds alignment, engagement and decision quality at every level.

Proven to improve delivery performance and accelerate the realisation of outcomes.

RISKWELL VERIFIED

Independent assurance of delivery capability and risk management that drives confidence in success.

Objective assurance of risk management effectiveness in a delivery context.

Evaluates capability, governance and performance – not just compliance.

Identifies strengths, gaps and improvement opportunities.

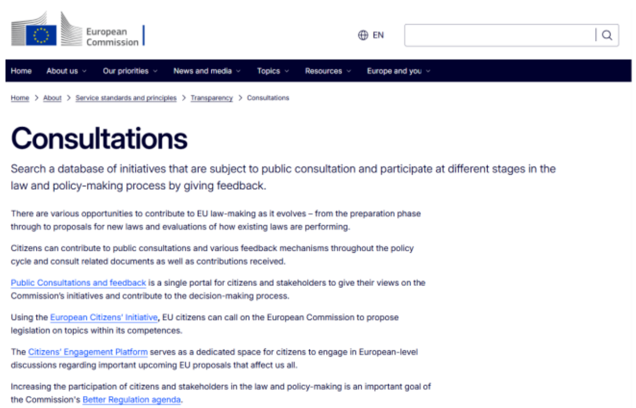
Strengthens delivery confidence for sponsors, stakeholders and boards.

Designed to lift delivery capability and increase the likelihood of success.

ONE ECOSYSTEM. ONE PURPOSE. The Riskwell and t2p partnership connects proven methodology, intelligent technology, independent assurance and people capability to help you deliver with confidence and achieve extraordinary outcomes.

EU Commission consultation

- What? e.g. EU AI Act or Digital Omnibus on AI (Kommissionsvorschlag vom 19. November 2025; provisorisch geeinigter Kompromisstext, Ratsdokument 9247/26 vom 13. Mai 2026)
- Who? everybody (individuals) and business stakeholders
- How? Website and feedback / comments possible in all 24 EU languages possible
- Why? Need to be reviewed in the law making process
- Only registration / or use of social media account necessary



t2p solutions oü
bringing trains2people

Thank you very much…
Vielen Dank…

t2p solutions oü
Katusepapi tn. 4/2
11412 Tallinn
(Estonia)

Wetzlarer Str. 8
D-35756 Mittenaar

Lars.Zimmermann@t2psolutions.com

M +49 172 7446456

www.t2psolutions.com