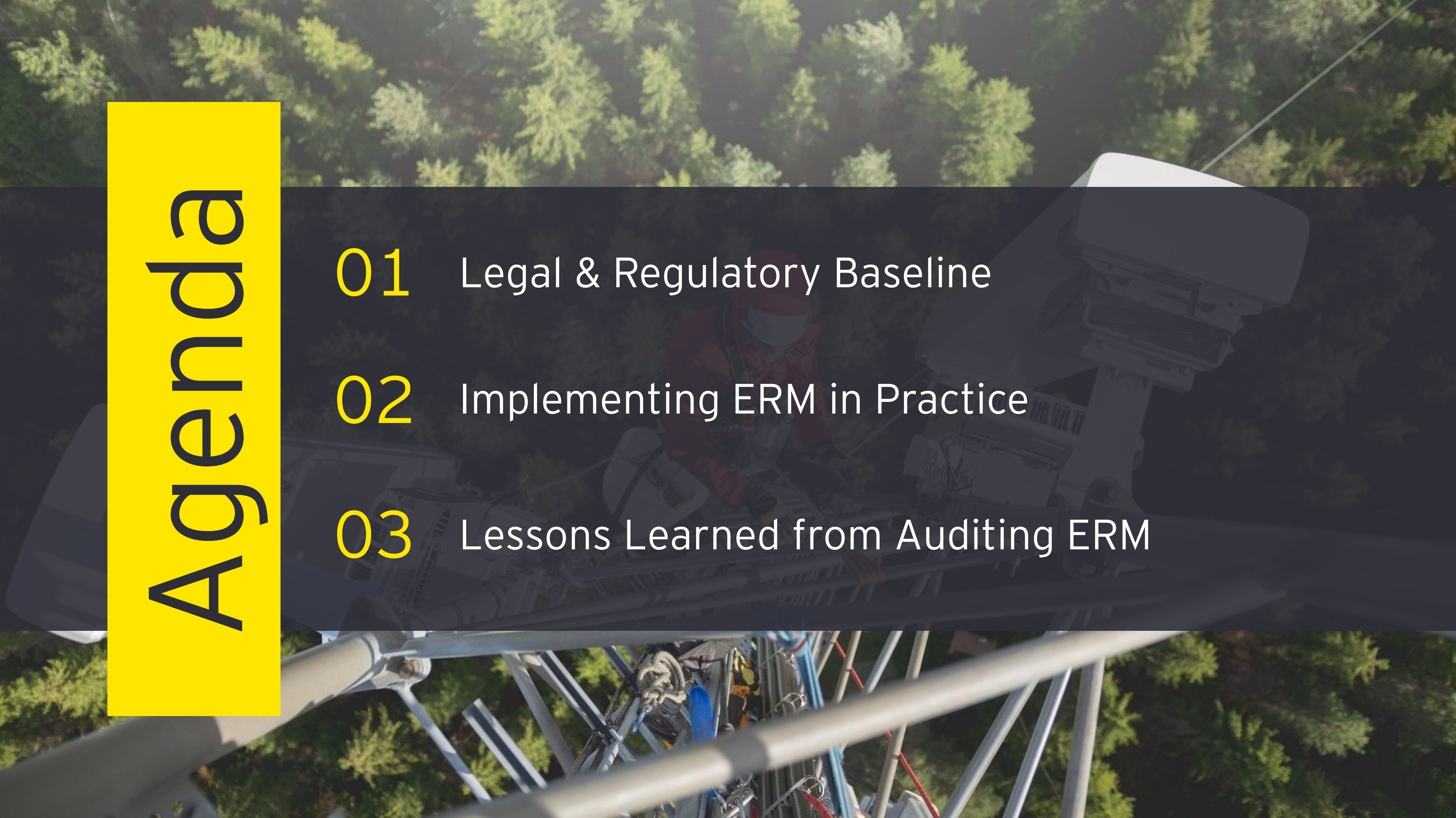
ERM in der Praxis

Netzwerk Risikomanagement

November 2023



Agenda

01 Legal & Regulatory Baseline

02 Implementing ERM in Practice

03 Lessons Learned from Auditing ERM

1

Legal & Regulatory Baseline

Legal & Regulatory Baseline for ERM (excl. Industry Specific Regulations)

Legal baseline for risk management in Switzerland (for companies subject to statutory audit):

- **OR art. 716a:** risk management is part of board oversight responsibility (no further specific requirements)
- **OR art. 961c:** companies need to inform about their risk evaluation approach as part of their annual report (specifically as part of the management report)
- **OR art. 728a:** companies need to have an Internal Controls System which also needs to be audited by the external auditor (existence of an ICS only. Effectiveness not specified)

Further standards, frameworks and guidelines that are/might be relevant for Swiss based companies:

- **Swiss Code of Best Practice for Corporate Governance:** provides more detailed requirements for risk management as part of the board oversight responsibility than OR
- **Richtlinien über das Risikomanagement Bund:** Swiss federation issued guideline which sets certain risk management requirements for its federal bodies and state owned organizations
- **ISO 31000 standard:** provides fundamental principles for the establishment of a risk management system and framework in organizations (this is what most of our clients actually refer to)
- **The Committee of Sponsoring Organizations of the Treadway Commission (COSO):** provides a comprehensive framework for Enterprise Risk Management (ERM) as well for Internal Controls (this is also what most of our clients refer to)
- **DIIR Revisionsstandard Nr. 2: Prüfung des Risikomanagementsystems durch die Interne Revision**
- **IDW PS 340 audit standard:** audit standard for early risk detection to audit against the legal requirements of § 91 Abs. 2 AktG (German law) to establish an early risk detection system. In Switzerland, these requirements have not (yet) been adopted, but some companies aim to voluntarily comply with the requirements of the IDW PS 340

2

Implementing ERM in Practice

ERM Framework Based on ISO 31000, COSO ERM and EY Good Practice

Business Resilience

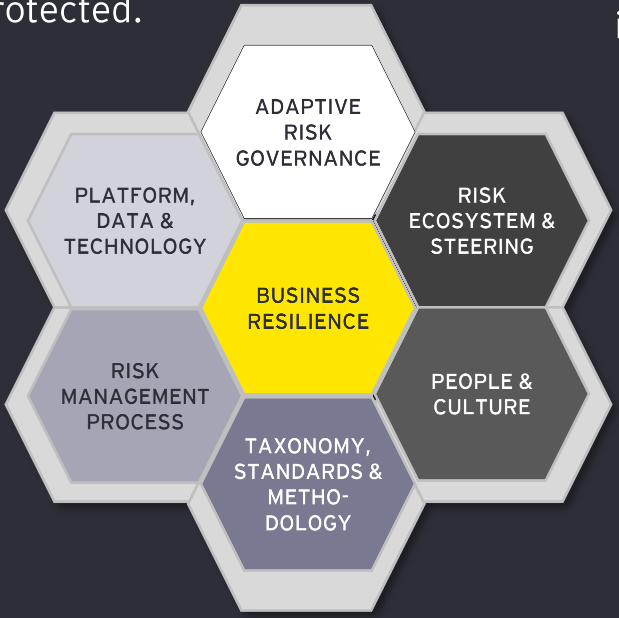
Identifies critical dependencies within your Risk Ecosystem and strengthens the vertical risk integration of risk management across risk-bearing objectives and key assets to be protected.

Platform, Data & Technology

Enables your Risk Management community to perform risk management activities in an integrated and efficient way based on a defined risk taxonomy and harmonized risk information across your risk management functions.

Risk Management Process

Defines the logical sequence of your risk management process activities of identifying & capturing, analyzing & evaluating, treating, reporting and monitoring risks throughout your organizational units.


ADAPTIVE RISK GOVERNANCE
PLATFORM, DATA & TECHNOLOGY
RISK ECOSYSTEM & STEERING
BUSINESS RESILIENCE
RISK MANAGEMENT PROCESS
PEOPLE & CULTURE
TAXONOMY, STANDARDS & METHO-DOLOGY

Adaptive Risk Governance

Defines the steering framework, the regulatory framework as well as the organizational framework based on a clear link between your Risk Strategy and its overall business objectives.

Risk Ecosystem & Steering

Integrates Upside, Downside and Outside Risks as part of your Risk Universe. The Risk Ecosystem together with the Risk Strategy serve as a basis for deriving the risk capacity and risk appetite framework as well steering-relevant Key Risk Indicators (KRIs).

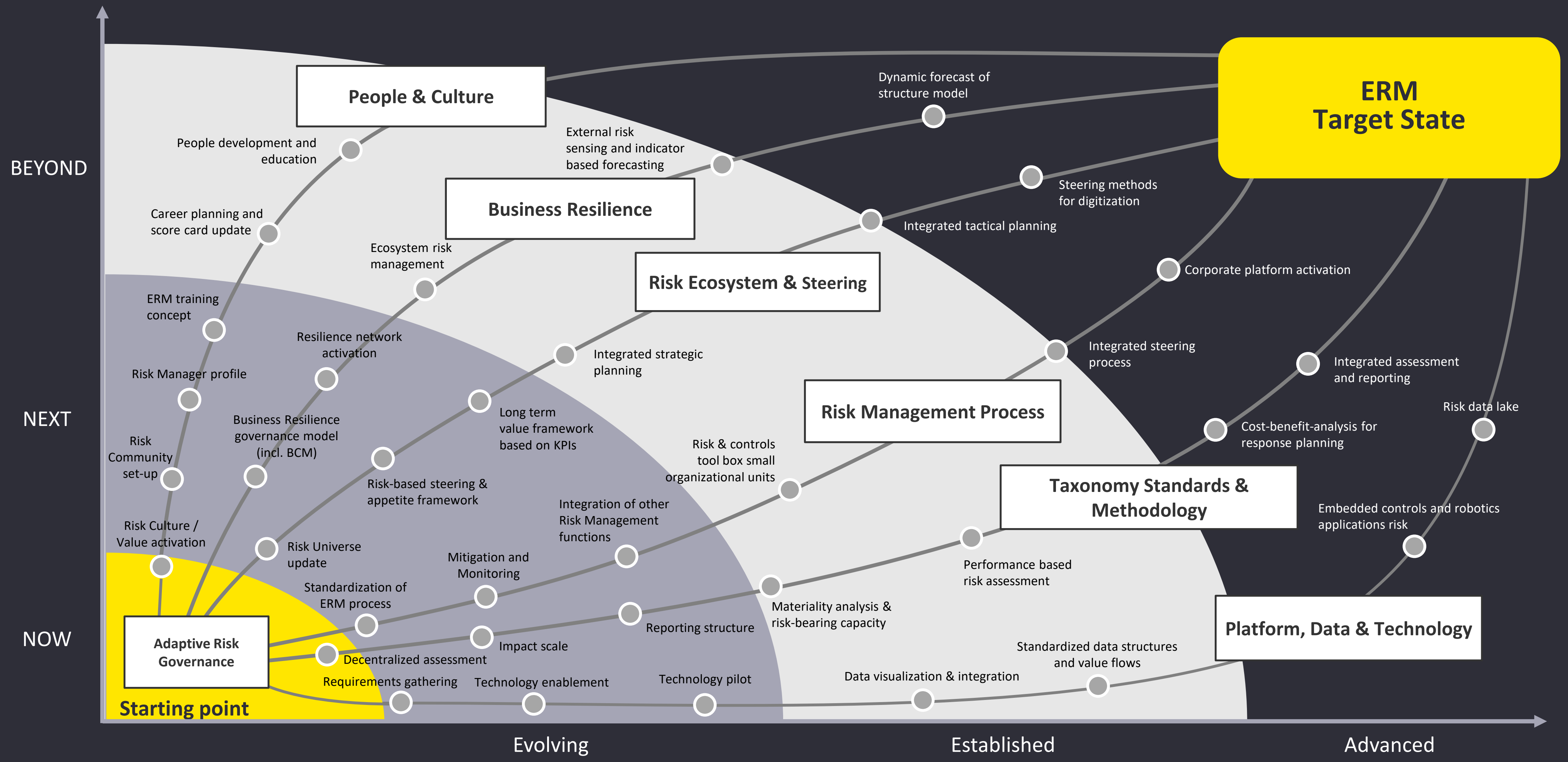
People & Culture

Driven by a clear allocation of tasks, competencies and responsibilities, Risk Culture refers to risk-aware decisions and behaviors infused by the culturalism in moments that matter.

Taxonomy, Standards & Methodology

Sets the baseline for a coherent company-wide risk management language, incl. defined terms and definitions as well as standards around criteria, scales and thresholds.

Illustrative ERM Maturity Development Journey



BEYOND

NEXT

NOW

Evolving

Established

Advanced

Starting point

Adaptive Risk Governance

People & Culture

Risk Culture / Value activation

Risk Community set-up

Risk Manager profile

ERM training concept

Career planning and score card update

People development and education

Business Resilience

Business Resilience governance model (incl. BCM)

Resilience network activation

Ecosystem risk management

External risk sensing and indicator based forecasting

Dynamic forecast of structure model

Risk Ecosystem & Steering

Risk Universe update

Risk-based steering & appetite framework

Long term value framework based on KPIs

Integrated strategic planning

Integrated tactical planning

Steering methods for digitization

Risk Management Process

Standardization of ERM process

Mitigation and Monitoring

Integration of other Risk Management functions

Risk & controls tool box small organizational units

Integrated steering process

Corporate platform activation

Taxonomy Standards & Methodology

Decentralized assessment

Impact scale

Reporting structure

Materiality analysis & risk-bearing capacity

Performance based risk assessment

Cost-benefit-analysis for response planning

Integrated assessment and reporting

Platform, Data & Technology

Requirements gathering

Technology enablement

Technology pilot

Data visualization & integration

Standardized data structures and value flows

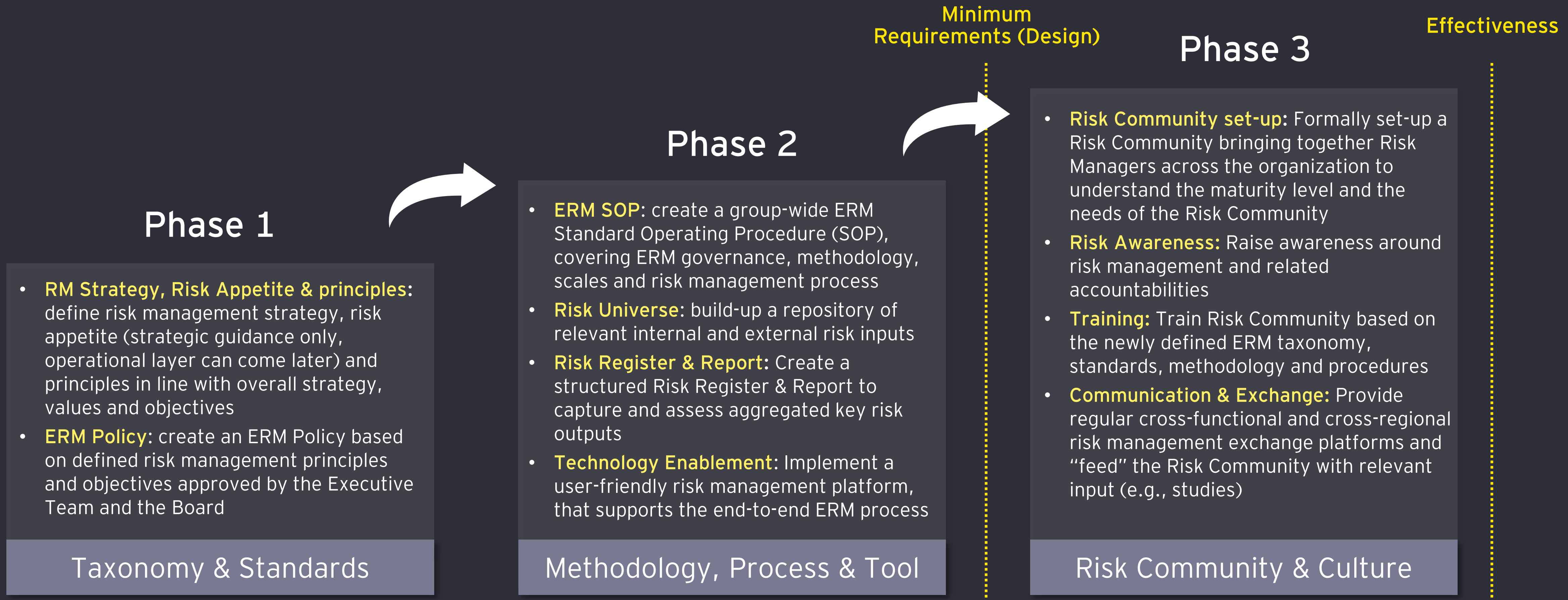
Embedded controls and robotics applications risk

Risk data lake

ERM Target State

Implementing ERM in Practice - Focus on Getting the Basics Right First

To build-up a holistic, yet pragmatic ERM program that is tailored to the organizational context, focus on getting the basics right first by building a solid framework foundation.



Minimum Requirements (Design)

Effectiveness

Phase 1

- **RM Strategy, Risk Appetite & principles:** define risk management strategy, risk appetite (strategic guidance only, operational layer can come later) and principles in line with overall strategy, values and objectives
- **ERM Policy:** create an ERM Policy based on defined risk management principles and objectives approved by the Executive Team and the Board

Taxonomy & Standards

Phase 2

- **ERM SOP:** create a group-wide ERM Standard Operating Procedure (SOP), covering ERM governance, methodology, scales and risk management process
- **Risk Universe:** build-up a repository of relevant internal and external risk inputs
- **Risk Register & Report:** Create a structured Risk Register & Report to capture and assess aggregated key risk outputs
- **Technology Enablement:** Implement a user-friendly risk management platform, that supports the end-to-end ERM process

Methodology, Process & Tool

Phase 3

- **Risk Community set-up:** Formally set-up a Risk Community bringing together Risk Managers across the organization to understand the maturity level and the needs of the Risk Community
- **Risk Awareness:** Raise awareness around risk management and related accountabilities
- **Training:** Train Risk Community based on the newly defined ERM taxonomy, standards, methodology and procedures
- **Communication & Exchange:** Provide regular cross-functional and cross-regional risk management exchange platforms and "feed" the Risk Community with relevant input (e.g., studies)

Risk Community & Culture

3

Lessons Learned from Auditing ERM

Audit Key Findings from & Watchouts for Reviewing ERM Programs

1 **Monitoring and follow-up on mitigation measures**: defined measures not being tracked and linked to budgeting cycle leading to reduced mitigation effectiveness

2 **Insufficient ERM documentation**: missing or incomplete ERM policies, procedures and operational documents

3 **Inconsistent level of risk awareness and maturity**: ERM taxonomy, methodology and process not being lived or consistently applied across the organization

4 **Lack of guidance & enablement**: lack of Risk Coordinator education, training and enablement (train the trainer) and insufficient technology platforms enabling the RM process

5 **Limited scope of risk assessment**: not covering all functions, units, regions and risk areas from a strategic, financial, compliance, operational and sustainability perspective

6 **Coordination & collaboration across assurance providers**: no integrated assurance approach across 2nd LoD and Internal Audit based on different methodology and taxonomy

Watchouts for ERM Audits

- **"Preaching for the own church"**: Internal Audit is often perceived to be close to risk management and as such to push their own agenda and priorities. To ensure acceptance and objectivity, it is thus key stay fact-based and unbiased
- **Ensure independence**: apply Chinese walls between ERM and Internal Audit teams or use third party assurance to ensure independence
- **Get the big picture**: involve key stakeholders from a 360° perspective (top-down and bottom-up) to get a holistic view on how ERM is lived across the organization

EY Risk Consulting Key Contacts

David Sütterlin

Partner, EY Risk Consulting

Basel, Switzerland

- Switzerland Risk Consulting Leader
- Enterprise Resilience and Risk Management Subject Matter Expert

> “
>
> Managing of risks is not only about risk avoidance – Companies need to shift their focus to embrace opportunities and disruption to be prepared for the day after tomorrow.

Patrick Erbsland

Director, EY Risk Consulting

Zurich, Switzerland

- Enterprise Resilience, ERM & BCM Solution Lead

> “
>
> Organizations that drive value generation, consider risk types holistically - aligned with the corporate strategy and development opportunities.

Ernst & Young

EY | Assurance | Tax | Strategy and Transactions | Consulting

About EY

EY is a global leader in assurance, tax, strategy, transaction and consulting services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. For more information about our organization, please visit ey.com.