Enterprise Risk Management and Emerging Risks

The Institute of Cost Accountants of India

Presented by
CMA Mrityunjay Acharjee

ENTREPRISE RISK MANAGEMENT

Enterprise risk management (ERM) is the process of identifying and addressing methodically the potential events that represent risks to the achievement of strategic objectives, or to opportunities to gain competitive advantage

ENTREPRISE RISK MANAGEMENT

Enterprise risk management (ERM) is a methodology that looks at risk management strategically from the perspective of the entire firm or organization.

It is a top-down strategy that aims to identify, assess, and prepare for potential losses, dangers, hazards, and other potentials for harm that may interfere with an organization's operations and objectives and/or lead to losses

ENTREPRISE RISK MANAGEMENT

ERM takes a holistic approach and calls for management-level decision-making that may not necessarily make sense for an individual business unit or segment. Thus, instead of each business unit being responsible for its own risk management, firm-wide surveillance is given precedence.

ENTREPRISE RISK MANAGEMENT

•Enterprise risk management (ERM) is a firm-wide strategy to identify and prepare for hazards with a company's finances, operations, and objectives.

•ERM allows managers to shape the firm's overall risk position by mandating certain bujsiness segments engage with or disengage from particular activities.

•Traditional risk management, which leaves decision-making in the hands of division heads, can lead to siloed evaluations that do not account for other divisions.

ENTREPRISE RISK MANAGEMENT

The importance of ERM is broad and far-reaching. A comprehensive ERM framework consolidates and improves risk reporting so you can identify key risks that may affect your organization, quantify and manage them better, and implement the proper controls to eliminate or reduce the threat.

ENTREPRISE RISK MANAGEMENT

The eight front components from top to bottom are :

Internal Environment,
Objective Setting,
Event Identification,
Risk Assessment,
Risk Response,
Control Activities,
Information & Communication, and
Monitoring.

WHAT IS ERM?

It is the capability to effectively answer the following quesions:

- Circular depiction is highly intentional
- Components are meant to be dynamic (reviewed back/forth in any sequence)
- Having the right culture is key

ENTREPRISE RISK MANAGEMENT

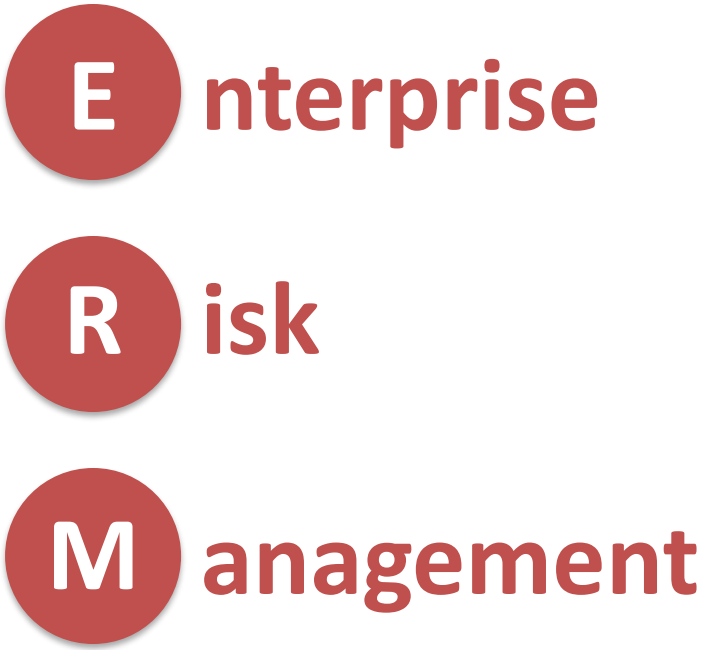
Enterprise risk management in business includes the methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives.

Highlights & Objectives

- **Understand** the importance of a Enterprise Risk Management
- **Identify Risks** to your mission / objectives / strategic plan
- **Evaluate** the likelihood and impact of risks
- **Learn** about emerging risks and best practices in mitigation
- **Assess** the overall risk & develop a practical response

Purpose

To provide a **summary of potential events** that may affect your organization and manage risks to **provide reasonable assurance** regarding the achievement of your mission and objectives.

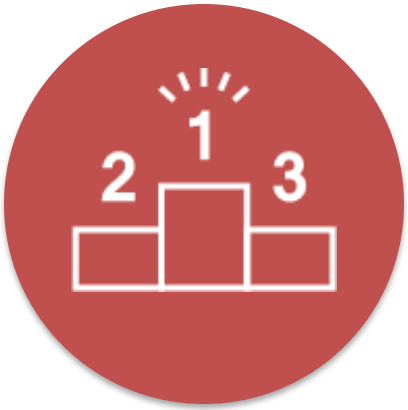


Why is ERM on the Rise?

- Regulator demands
- Unanticipated risk events affecting the organization
- Emerging best practice expectations
- Emerging corporate governance requirements
- Board of Director requests

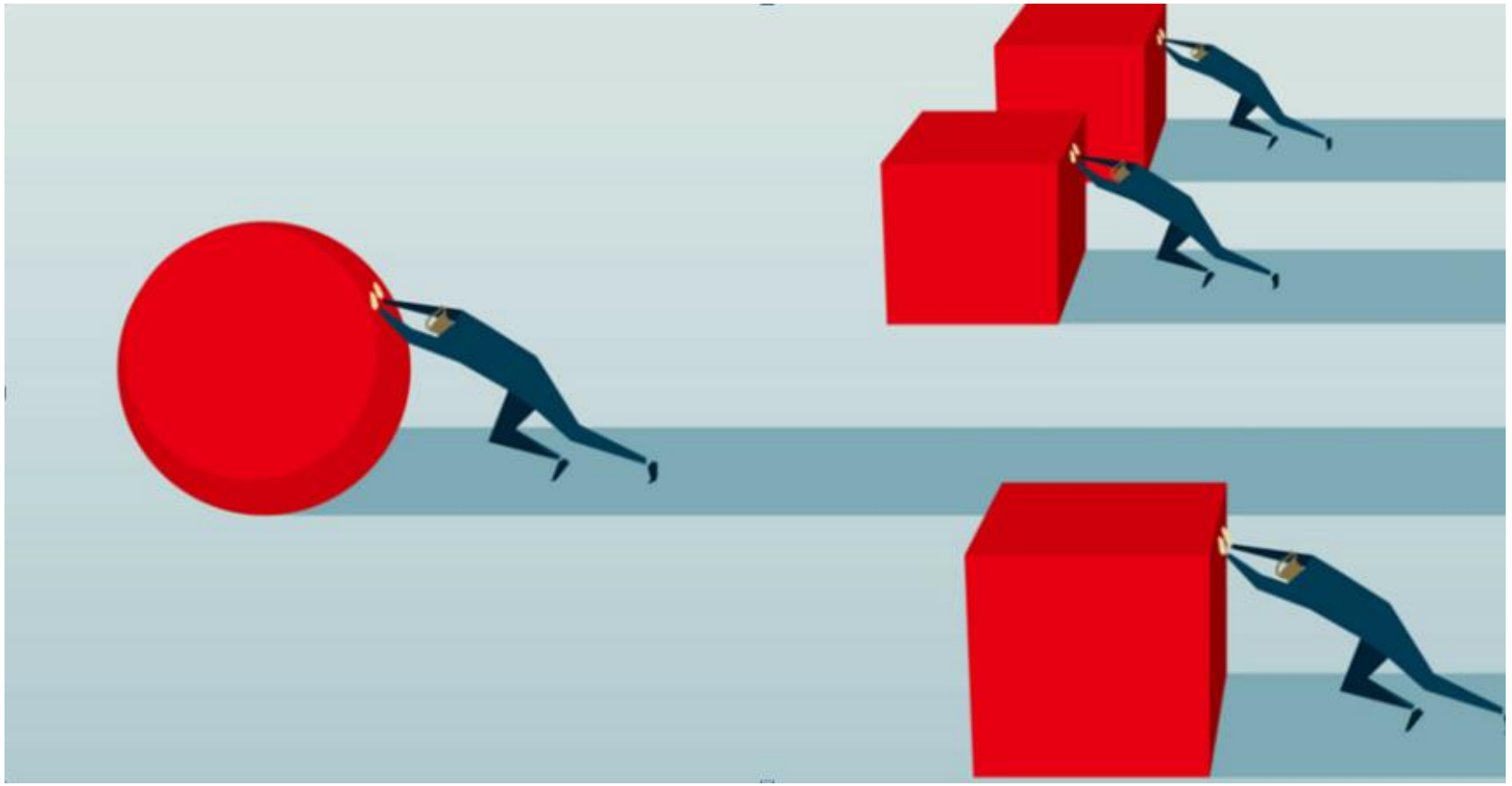
Why is this Important?

It is a proven methodology to capture your risks and visually rank them so your organization can make informed decision on how to spend your budget dollars.

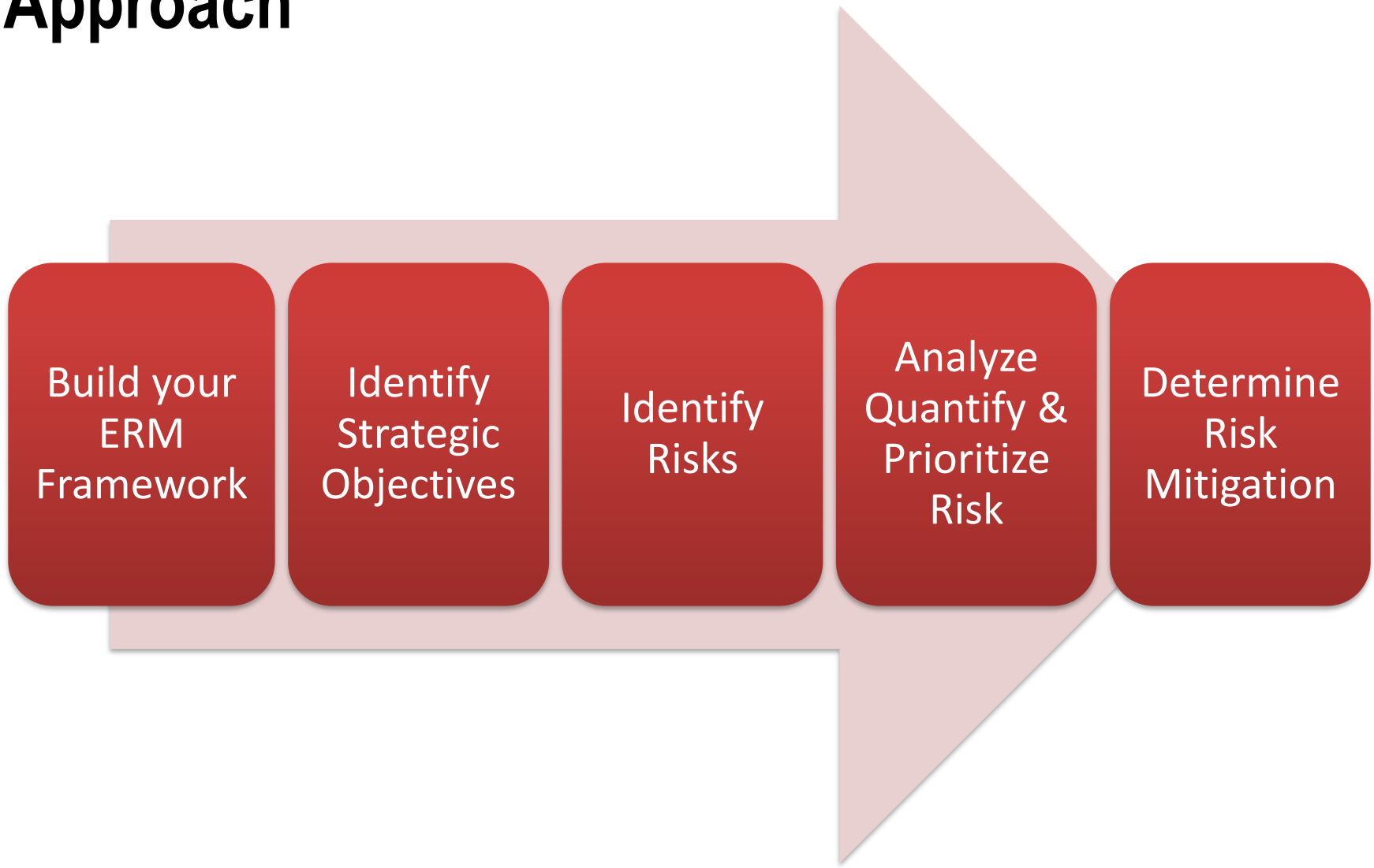


Priorities

Work Smarter – Not Harder



Approach


Build your ERM Framework
Identify Strategic Objectives
Identify Risks
Analyze Quantify & Prioritize Risk
Determine Risk Mitigation

Build your ERM Framework

Building a Framework

Things to consider when building your framework

- Framework – ISO vr COSO
- Where to Start – Full rollout? Phased approach?
- What Model to implement- Risk factor vrs objectives based?
- ERM Organizational position - CRO, CAE, Risk Manager, Risk Committee?

Identify Objectives

Tie into strategy and mission

Example Risks to Objective Categories

- Collaboration Risk
- Management & Operational Risk
- Financial Risk
- External & Reputation Risk
- Personnel & Volunteers Risk
- Grant Risk

Brainstorm Risks Events

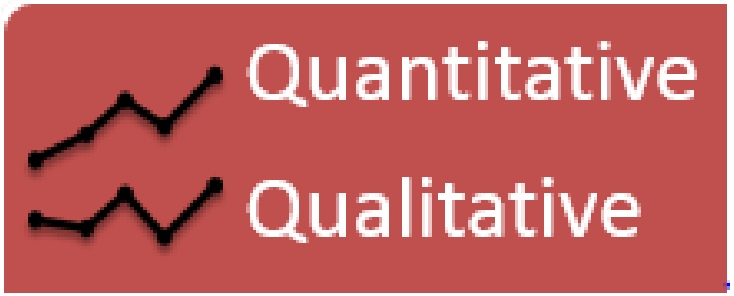
Risk Event Identification Techniques

May include a combination of different types of techniques combined with supporting tools:

- Event Inventories
- Internal Analysis & Surveys
- Process Flow Analysis
- Current Events
- Facilitated Workshops and Interviews

Analyze, Quantify & Prioritize Risk

Methods to Rank Risk



Qualitative

A qualitative analysis would use a scale of "Low, Medium, High" to indicate the likelihood of a risk event occurring.

Quantitative

A quantitative analysis will determine the probability of each risk event occurring. For example, Risk #1 has an 80% chance of occurring, Risk #2 has a 27% chance of occurring, and so on.

Our discussion will focus on **qualitative analysis**

Develop Risk Analysis Matrix

Develop a **risk mapping for impact and likelihood** to help determine which risks need risk response. For example:

	Likelihood				
Impact	**Rare**	**Unlikely**	**Possible**	**Likely**	**Certain**
Catastrophic	moderate	moderate	high	critical	critical
Major	low	moderate	moderate	high	critical
Moderate	low	moderate	moderate	moderate	high
Minor	very low	low	moderate	moderate	moderate
Insignificant	very low	very low	low	low	moderate

Types of Risk Impact

In order to align discussions around why risk are significant and what should be done about them, you should consider dividing your analysis in to types of impact:

Strategic
Causes a strategic objective to fail

Financial
Incurs unanticipated costs or reduces revenues

Operational
Affects the quality or efficiency of how work gets done

Reputation
Creates negative media attention

Environmental, Health and Safety
Jeopardizes staff, volunteers or others' well-being

Legal
Triggers arbitration or litigation against your organization

Technology
Exposes application, data, operating systems, network or infrastructure to inappropriate access/change

Example of a Risk Rating

Category	Risk	Risk Impact	Probability	Impact	Risk Level
Personnel/Volunteers Risk	Harm reputation of your organization	Reputation	Possible	Catastrophic	High
Grant Risk	Delays in disbursement	Financial	Possible	Moderate	Moderate
Personnel/Volunteers Risk	stolen credentials leads to cyber incident	Technology	Likely	Major	High
Collaboration Risk	Loss of identity	Strategic	Rare	Major	Low

Determine Risk Mitigation

Determine Risk Mitigation

Reduce / Mitigate risk

Activities with a high likelihood of occurring, but impact is low.

Eliminate / Avoid risk

Activities with a high likelihood of loss and high impact.

Share / Transfer risk

Activities with low likelihood of occurring, but with a high impact.

Accept risk

If cost-benefit analysis determines the cost to mitigate risk is higher than cost to bear the risk.

Risk mitigation - Insurance

- Risk transfer involves moving risk to 3rd party via contractual arrangement

- Insurance is most common Risk Transfer mechanism

- Outsourcing: risk transfer financial offset – pre incident assessment planning. loss control property/cyber penetration testing.

Risk Examples

Example Category - Personnel/Volunteers Risk

- Injury at work
- Cause your organizations client injury
- Harm reputation of your organization
- High turnover
- Triggers a cyber security incident

Example Category - Financial Risk

- Inaccurate and/or insufficient financial information
- No financial planning (budgeting)
- Lack of financial liquidity
- Poor pricing policy (e.g., overpriced activities in grant applications)
- Excessive indebtedness
- FX losses
- Financial fraud
- High transactional costs
- Inadequate maintenance of long-term sources of funding
- Inadequate reserves and cash flow
- Dependence on a low number of revenue sources
- Inadequate investment policy
- Inadequate insurance coverage
- Funds used against the intent of donor/grantor

Example Category - Operational Risk

- Not enough beneficiaries
- Not enough well-trained Personnel
- Uncertainty about security of assets
- Competition from other organizations
- Dependence on suppliers (their strong bargaining power)
- Ineffective fundraising system
- Lack of formalized procedures
- Inefficient and ineffective IT system
- Implementing activities in a dangerous environment
- Natural disaster, fire, flood, theft
- Deviation from core mission “in search of” funding sources

Example Category - Management

- Inadequate organization structure
- Management lacks adequate experience or not well organized
- Management dominated by individual leaders
- Resignation of key personnel
- Conflict of interest
- Ineffective communication System
- No direction, strategy, and plans

Example Category - Grant Risk

- Delays in disbursement
- Lack of knowledge and skills to utilize the awarded grant
- Changes in environment preventing utilization of the awarded grant
- Undervalued contract

Emerging Risks: Privacy / GDPR

Are you ready for the General Data Protection Regulation (GDPR)? GDPR is the most important change in privacy in 20 years taking effect May 25, 2018.

In the future, aspects of the European GDPR are likely to find their way into other regulation as well, organizations should start to prepare their policies and procedures for this.

GDPR - Overview

- Introduction
- GDPR Requirements
- Penalties
- How it may impact companies
- What companies can do to comply

What is the GDPR?

European Union's new framework for data protection law replaces the 1995 Directive

One Stop Shop – EU "main establishment" of controller works with Lead Supervisory Authority

Application to Companies Worldwide - Simply offering products to and/or collecting data about persons in the EU is enough for the law to apply- Applies to Data Controllers and Data Processors

Effective Date – May 25, 2018

What is the GDPR? (cont'd)

- Principle Based – Purpose limitation, data minimization, accuracy, storage limitation, integrity and confidentiality, accountability
- Lawful Basis Required for Processing Personal Information
- Greater Protections and Rights to Individuals in the EU
- Privacy Information must be clearly communicated
- Data Protection Officers (regular and systematic monitoring on a large scale, or sensitive data, or public body); Associations representing categories of controllers MAY designate a DPO for their Controllers
- Appropriate security of Personal Data

GDPR: Penalties, Complaints, Reputation

Penalties

- **20 million euro or up to 4% of total worldwide annual turnover, whichever is higher**
- Member States can impose additional fines not covered by Art. 83

Complaints/Investigations

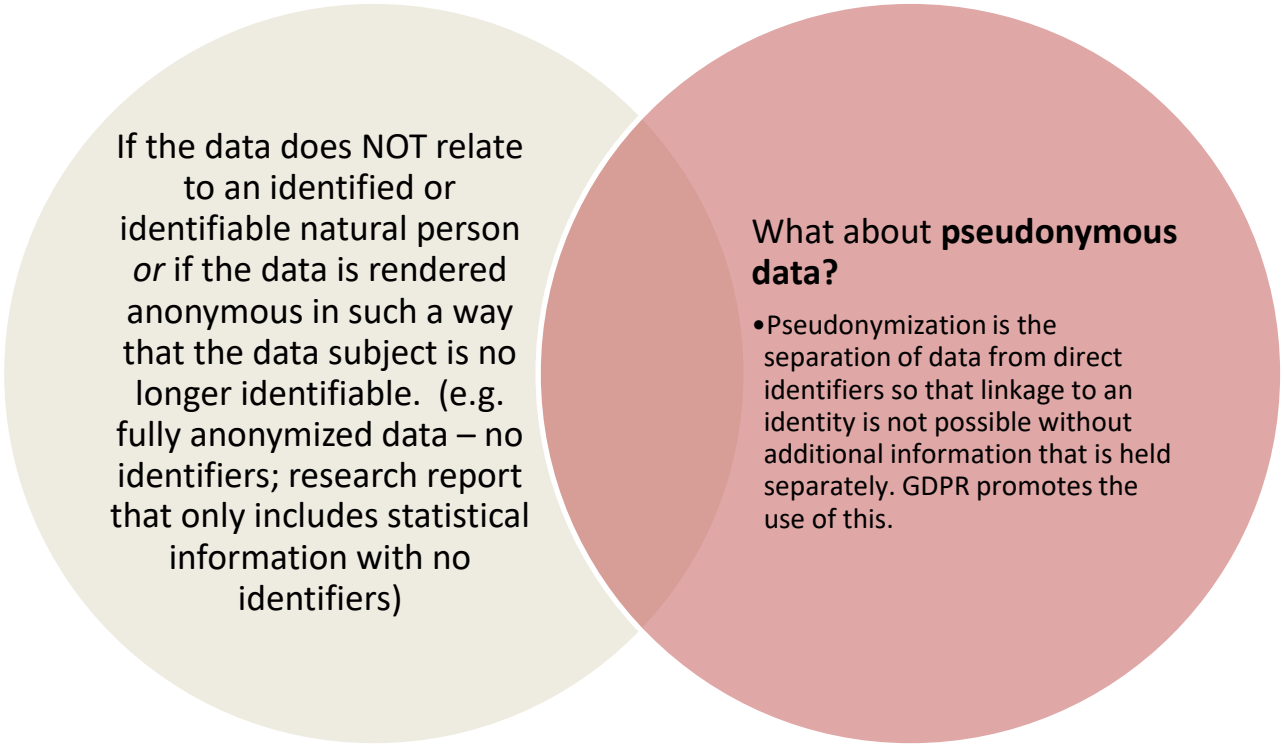
Reputational Consequences

GDPR applies……

When a company processes an EU data subject's information if the processing is related to:

- *offering or providing goods or services - even if no* payment is required
- *monitoring individuals in person or online*

GDPR does not apply…



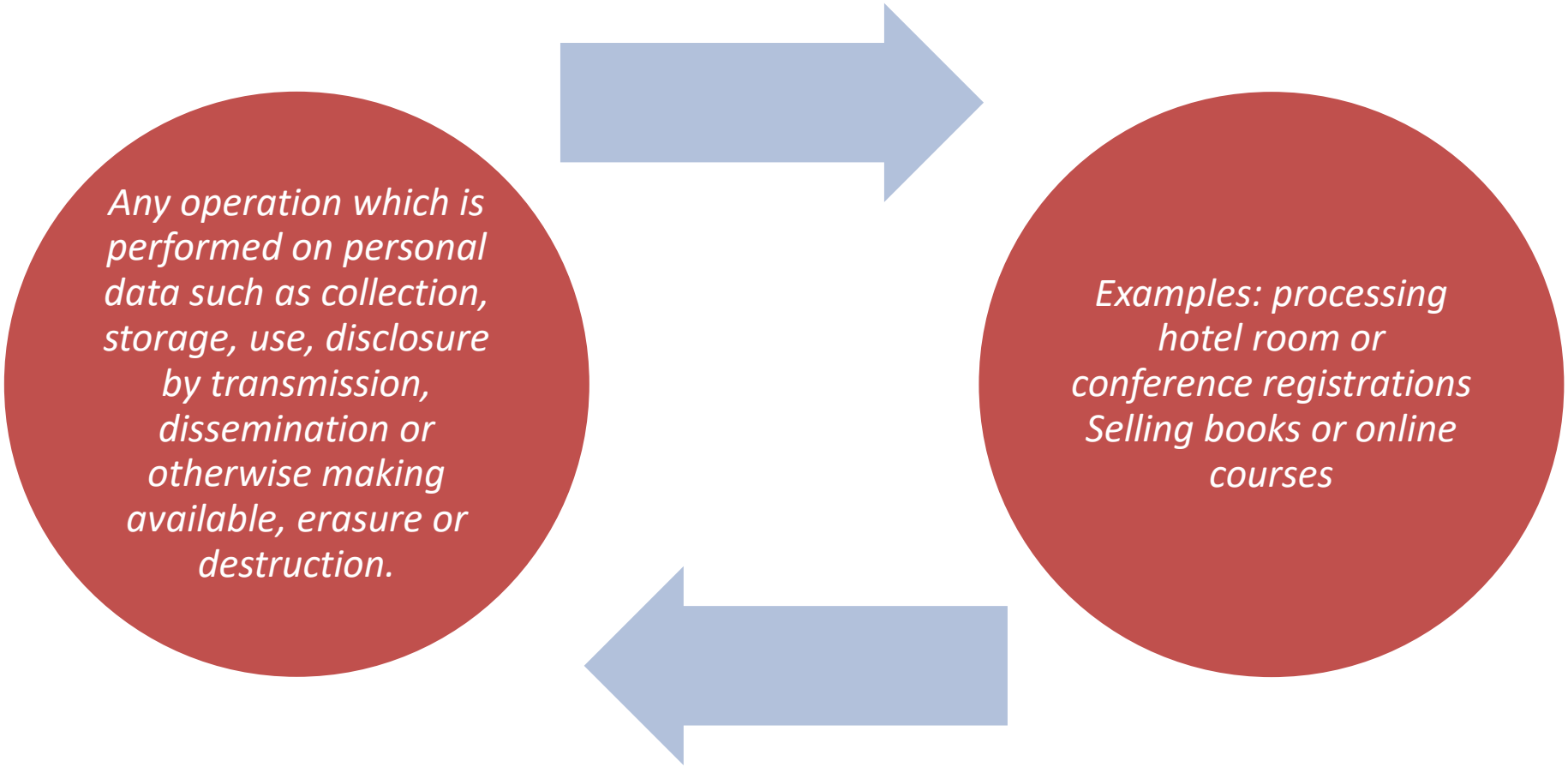
GDPR: Controllers and Processors

Controller: company that alone or jointly with others determines the purposes and means of processing of personal data

Joint Controller: When two or more controllers determine the purposes and means of processing

Processor: processes data on behalf of the controller

GDPR: Processing



GDPR: What is Personal Data?

"Personal data" is any information which relates to a living individual who can be identified:

- From that information
- From that information combined with other information held or likely to come into the possession of the company

Examples

- ✓ Name
- ✓ Postal or work or email address
- ✓ Phone number
- ✓ ID numbers (e.g. passport, license)
- ✓ Location data (usually from devices)
- ✓ **Bank account details**
- ✓ Expressions of opinion
- ✓ Photographs, sound recordings, film
- ✓ IP addresses
- ✓ Information stored in cookies or similar technologies
- ✓ Training records

GDPR: What is Sensitive Data?

"Sensitive data requires special handling, higher protections

Not specifically defined under the GDPR so Member States can regulate further

GDPR prohibits their processing unless exemptions are in place: explicit consent, employment obligations, etc.

Examples

- ✓ Biometric data
- ✓ Health and genetic data (allergies)
- ✓ Employment data
- ✓ Criminal convictions
- ✓ Racial or ethnic data
- ✓ Political opinions
- ✓ Religious or philosophical
- ✓ Trade-union membership
- ✓ Sex life or sexual orientation

GDPR: Key Changes

1	Data Subject Rights	Increased transparency and creating new rights. Right to Access, Right to be Forgotten, Data Portability
2	Consent	Consent for processing must be freely given, specific, informed and unambiguous. Strict Requirements – see Art. 29 WP Guidance
3	Data Processors and controllers	More contract requirements to be flowed by controllers to processors (data processing agreements)
4	Data Protection by Design (DPbD)	DPbD is about ensuring that privacy is embedded throughout the organization and being able to demonstrate compliance to regulators
5	Cross-Border Transfers	This privacy-compliant cross-border data transfer strategy must have “adequate protections”
6	Data Breach Notifications	Controllers required to notify competent supervisory authority and, in certain cases, also to affected data subjects. Generally within 72 hours.

GDPR: Security Requirements

Flexible requirement that takes into account several factors: (1) state of the art; (2) implementation costs; (3) nature, scope, context and purposes of processing; (4) risk of varying likelihood and severity for the rights and freedoms of natural persons

Breach notification requirement: 72 hours or without undue delay

Specific callouts for: encryption, pseudonymization, backups, procedures for regularly testing/assessing/evaluating effectiveness of security measures

GDPR: What Companies Can Do To Comply?

Organization:

- Assemble Your Team
- Roles & Responsibilities
- Know your data
- Security Obligations

Processes:

- Determine Systems tied to Data
- Employee Outreach
- Collaboration
- Training

Monitor & Enforce:

- Encourage Communication
- Make Good Conduct Visible
- Manage Employee Error

Document:

- Privacy Policy
- Security Policies
- Breach Response Plan
- Document Retention Plan

GDPR: Data Governance

Data Governance

- **Policies** – data governance policy with data classification scheme
- **Processes** – roadmaps for determining governance steps
- **Data Mapping and Inventory** – required to document all data processing activities in lieu or notifications/approvals to DPAs
- **Vendor Management** – who has data, where is it, and how managed

GDPR: Contracts for Using Processors

Processor must provide contractual guarantees that they use data security technology and methods that meet GDPR

Gap analysis and legal review of contracts and determine if amendments need to be made to meet GDPR requirements

Make amendments in order to continue using Processor in compliance with new requirements

GDPR: Data Transfers

Only one part of GDPR compliance – still many other compliance requirements

Options – need to have "adequate data privacy protections"

- **Standard Contractual Clauses**
- **Privacy Shield** - **Not for Trade Associations, Other nonprofits, No Banks (must have FTC jurisdiction)**
- **Binding Corporate Rules** (GDPR gold standard, but complex)
- **Country deemed by EU as having "adequate protections"** (Argentina, Canada, Israel, New Zealand, Switzerland, Uruguay - NOT US)

GDPR: Standard Contractual Clauses

What are Standard Contractual Clauses?

Pre-approved contractual language to be incorporated into agreements, unchanged.

Two sets of standard contractual clauses for transfers from data controllers to data controllers established outside the EU/EEA and one set for the transfer from controllers to processors established outside the EU/EEA.

GDPR: Data Transfer Exceptions

Consent – must be informed, explicit, more complex under GDPR

Contract – must be necessary for performance or conclusion of a contract or implementation of pre-contractual measures taken at the data subject's request

Public interest

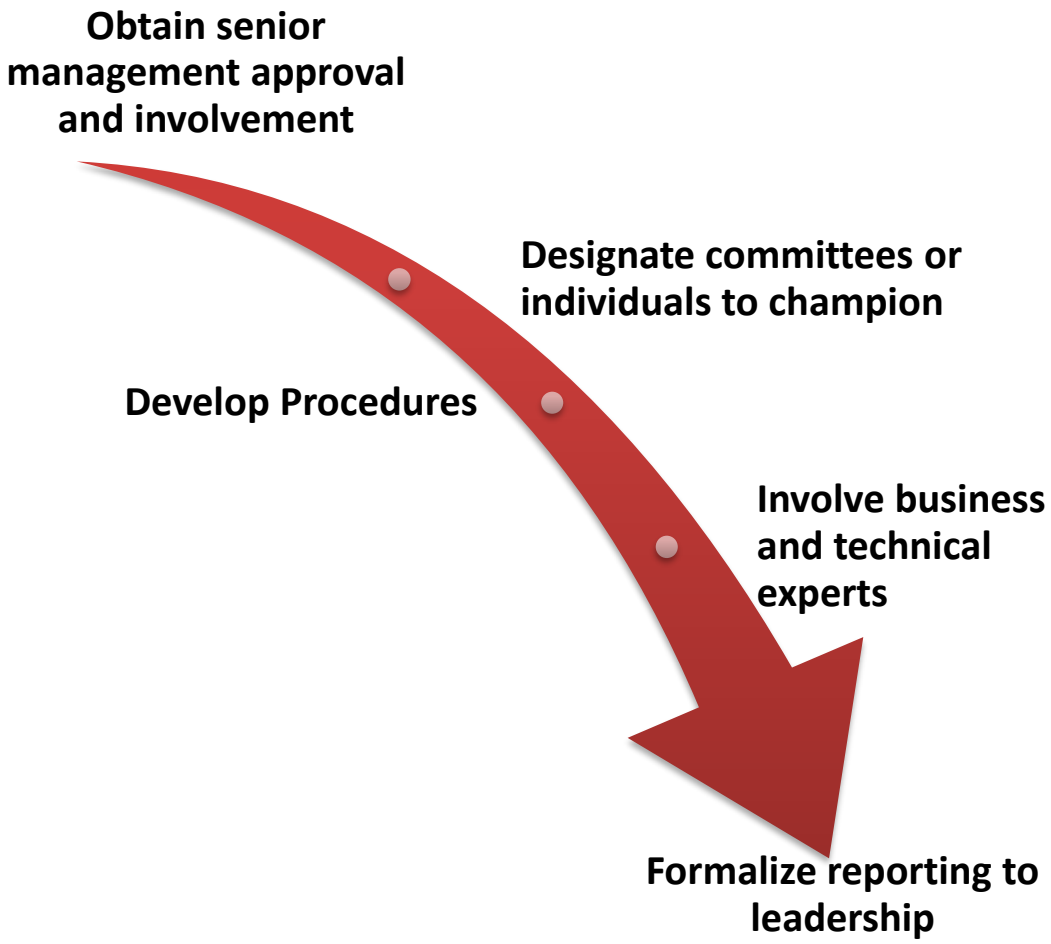
Legal claims - necessary for the establishment, exercise, or defense of legal claims

Vital interests – necessary to protect the vital interests of data subject or of other persons (if data subject is physically or legally incapable of giving consent)

Emerging Risks: Culture and Conduct

> “It takes 20 years to build a reputation, and five minutes to ruin it. If you think about that, you’ll do things differently.”
>
> -Warren Buffett

ERM - Critical Success Factors

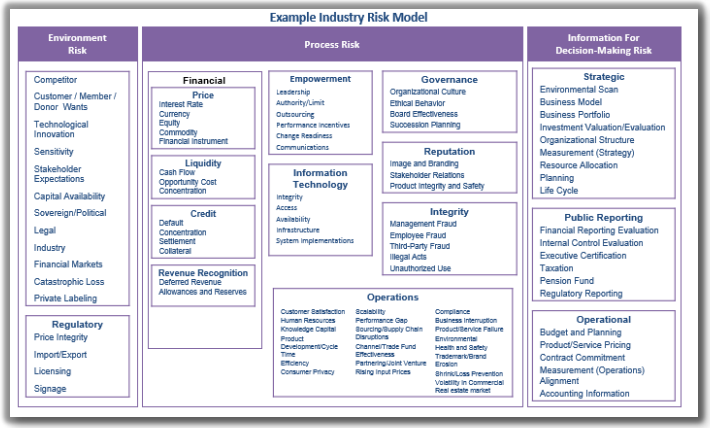


Develop ERM Procedures

Formalize Risk Reporting

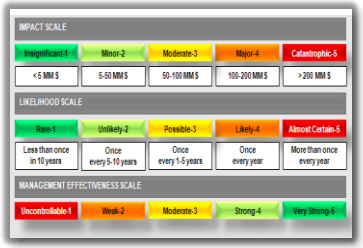
1 Updated Risk Universe

- Enterprise Universe
- Survey Results

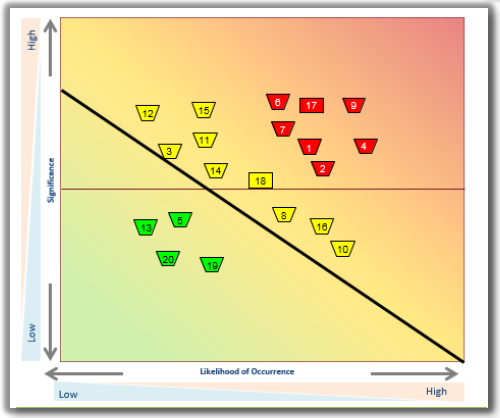


2 Risk assessment criteria

Use risk assessment criteria to prioritize risks – identify the most significant risks to the organization

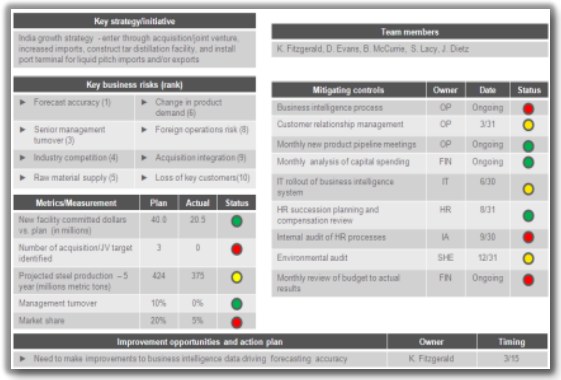


3 Prioritized risk heat map



4 Mitigation Plans

Identify risk mitigation plans for top 10 most significant risks



ERM and Internal Audit

Thank You