corix partners

Building meaningful, data-driven decisions around Risk

A Structured Approach to Risk Management and Modelling

December 2023

Managing Risk or managing risks?

Over the past 20 years, **Corix Partners** and the consultants in its network have been assisting large firms in building effective risk management models.

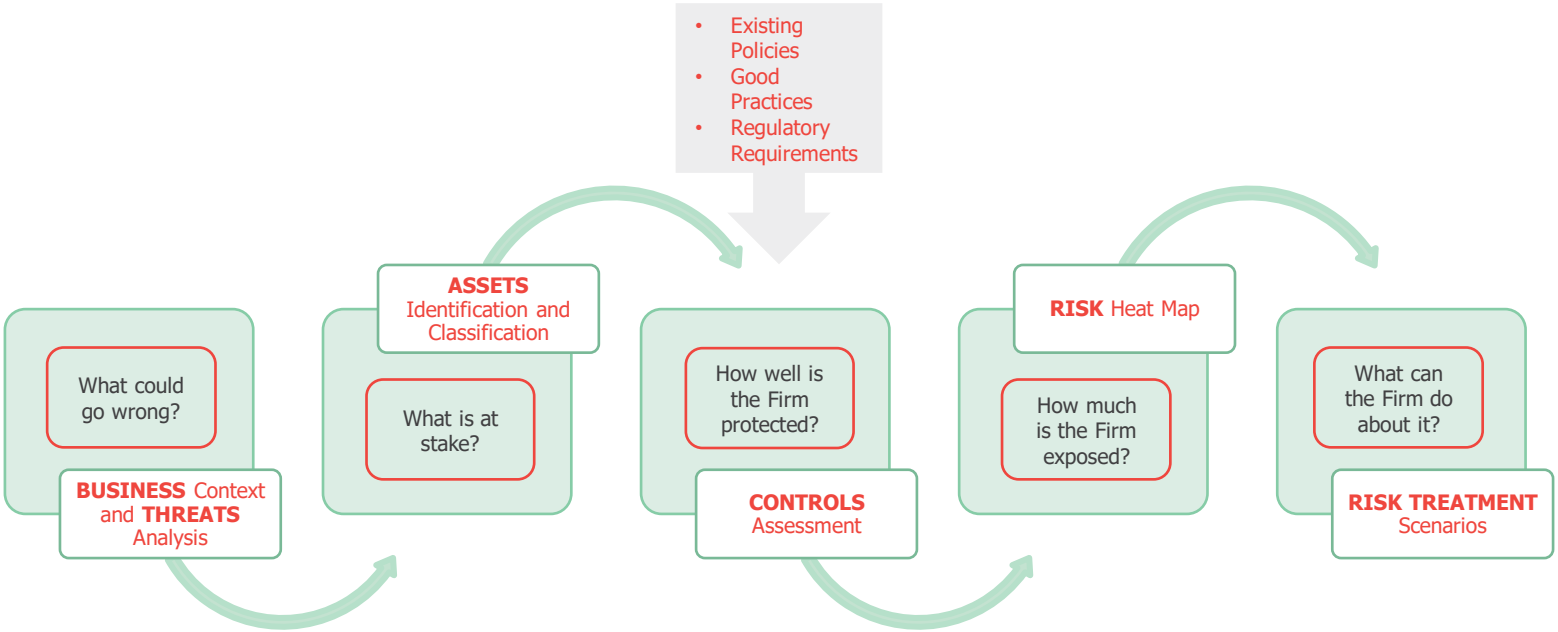
All too often, we come across situations where those have been built around qualitative perceptions, leading to large number of meaningless "risks" being handled through "ivory-towered" risk registers in complete isolation from the reality of the business, the threats it faces, or the protective measures that are – or are not – in place.

We believe that **Risk** can be managed only through the sound understanding of the threats the business is facing, the assets it needs to protect and the level of protection it can afford for those assets.

We have developed a structured, quantitative, data-driven approach rooted in the reality of each asset – its nature, its criticality to the Business and its actual level of protection against Threats – to assist business stakeholders in making actionable decisions around Risk Treatment.

From understanding the Business context to managing Risk

A Structured Approach to Managing and Modelling Risk



Business, Threats and Assets

In our view, every Firm should conduct periodic evaluations of the **Threats** it faces in relation to the nature of its Business, the specifics of its industry sector, or the geographies in which it operates

The term **Asset** is used to designate the targets the Business wants to protect from the identified Threats

- They can be digital (e.g. IT applications or systems), physical (e.g. offices or data centres) or hybrid (e.g. bank branches or call centres)
- The nature and structure of each Asset must be assessed in order to determine the most appropriate level of protection

Assets will vary not just in nature but also in their relative importance to the Business

- Assets must be classified by the Business in terms of criticality in order to focus attention and resources on the protection of the Assets which are most critical to the Business
- This step must remain simple and effective, as this is just the start of the risk management process – and certainly not its only aim: High criticality does not mean high Risk if the Asset is well protected.

Controls Assessment

Protecting Assets from the **Threats** which may target them is achieved through the implementation of practical measures ("**Controls**") that have a protective effect and can be mandated by policy, adherence to good practice or regulatory compliance

Controls work in different ways and can be grouped broadly into 2 categories :

- **Preventative** Controls, which reduce the Likelihood of Threats affecting Assets
- **Mitigative** Controls, which reduce the Impact Threats can have on Assets

Controls can be mapped to types of Assets (based on their nature and structure), to the classification of each Asset, to the Threats and (if necessary) to specific policies, good practice models or regulatory frameworks

A structured **Assessment** of the presence or absence of the mandated Controls for each Asset is the only way to determine how well the Asset is actually protected

- On grounds of efficiency, Controls common to multiple Assets such as those applying to infrastructure services (e.g. networks or data centres), or common service providers (e.g. major Cloud players), can be assessed once, and the results of such Assessments re-used for each associated Asset as "building blocks" of the Asset's Assessment
- A scoring mechanism allows the determination of Compliance scores for each Asset against the mandated Controls

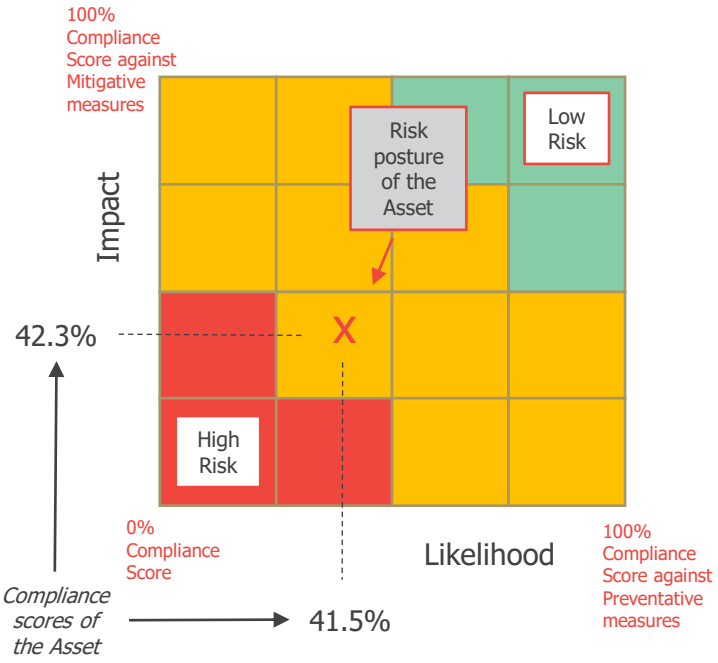
Risk Heat Map

The level of **Risk** carried by an Asset results from the presence or absence of Controls to protect the Asset from the Threats that may target it

- Assets with a high Compliance score against mandated Controls are well protected and carry a low Risk level

The grouping of Controls in Preventative and Mitigative categories allows the determination of Compliance scores in both dimensions, effectively equivalent to the Likelihood and Impact dimensions of a Risk Matrix

- A quantitative Risk Heat Map can be drawn as a result and Asset Assessments scores plotted on it
- The colour-coded background of the Risk Heat Map can be determined with Business stakeholders on the basis of their Risk appetite and the layout of the matrix itself can be adjusted to match existing practices

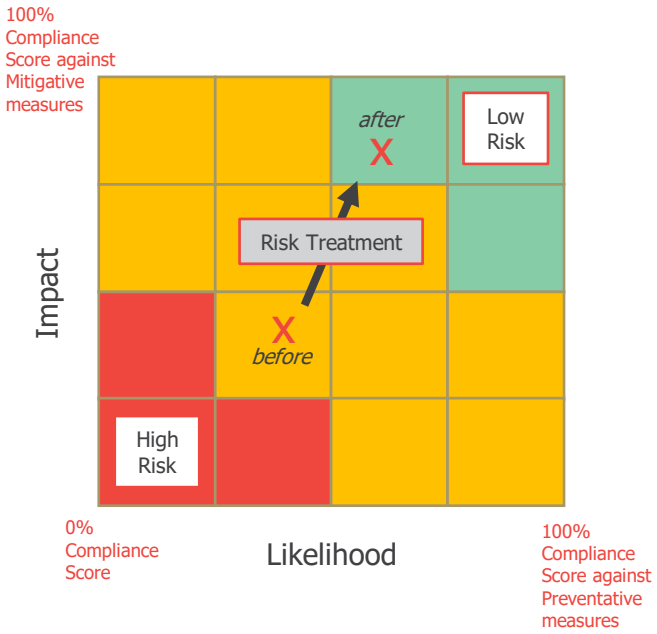


Risk Treatment (by Asset)

Risk Treatment is the process by which the Risk posture of an Asset is improved through the implementation of additional Controls

The Risk Heat Map can be used to visualise the effect the Risk Treatment is having on the Risk posture of the Asset

- Compliance scores in both dimensions evolve as additional Controls are implemented to reflect the increased level of protection of the Asset



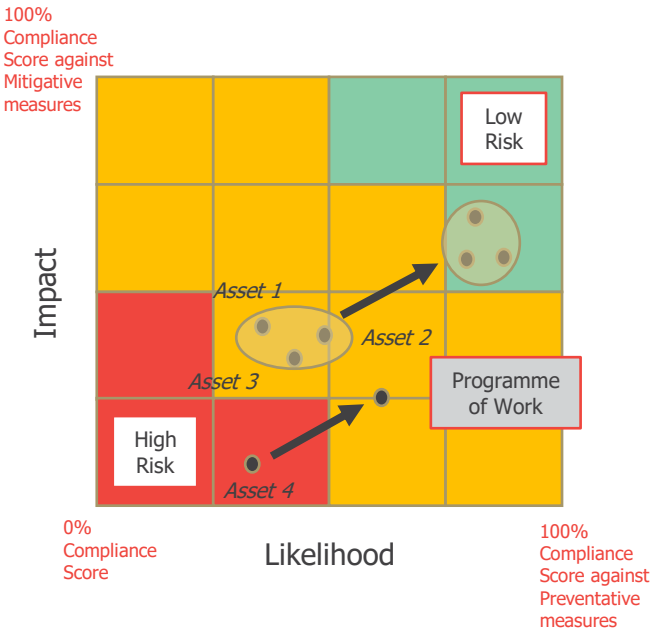
Risk Treatment (Firm-wide)

Assessment results can be aggregated for all Assets across the Firm, or by Business Unit, Division or Geography

- It is essential to match the level at which decisions will actually be made around Risk Treatment by Business stakeholders

It allows the visualisation of outliers and the effect of larger Programmes of Work can also be plotted on the Risk Heat Map to show how they would improve the actual level of protection of the Business

- The mapping of Controls to Threats could also allow the determination of Compliance scores by Threat across Firm, Business Unit, Division, or Geography, and the plotting of the results by Threat instead of Asset

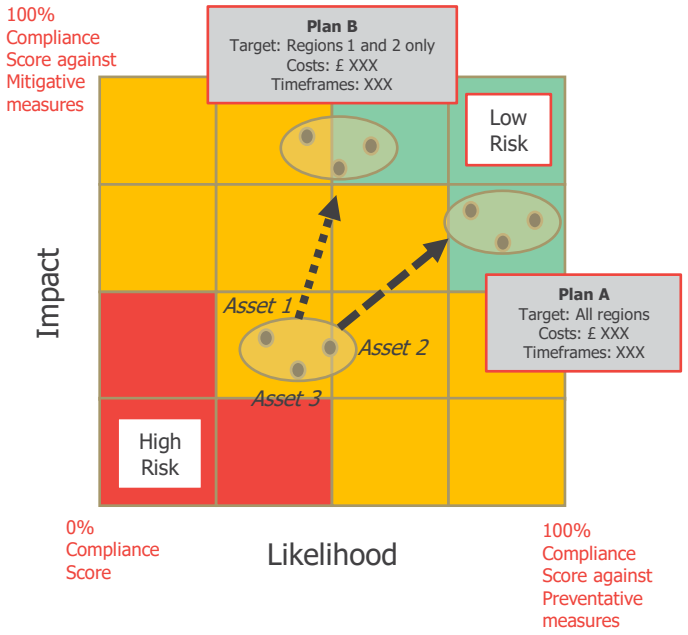


Risk Treatment (Simulations)

The same visualisation technique can be used to run simulations ("What-If" scenarios) and allow Business stakeholders to select the most effective Risk Treatment Scenarios in relation to resources or timeframes available

It gives Business stakeholders a platform to answer real management questions around Risk on a quantitative and data-driven basis

- What amount of Risk reduction will I achieve in return for a given investment over a given timeframe?
- Will it be sufficient to bring my operations within Risk Appetite from a business or regulatory standpoint?



Contact us

Corix Partners Limited

Registered in England and Wales (No. 06774109)
VAT Reg ID: GB970 2205 45

269 Farnborough Road
Farnborough, Hampshire,
GU14 7LY
United Kingdom

contact@corixpartners.com

www.corixpartners.com

@corixpartners