

# Risk Mitigation Analysis (RMA)

- **Purpose:** Its purpose is to identify and categorize the cyber risks in ways that will inform the implementation of the strategy. The RMA is related to business alignment, to the organization's threat profile and is a predicate to other activities related to the assessments. It is the second element of any cybersecurity activity and should follow a yearly review / refresh to stay current and relevant to the business conditions. Companies often engage in compliance without knowing where to start to best match limited resources to highest benefit. They also may not be aware of their threat profile, that their cyber risk is so acute that the company's very existence can be in jeopardy. The RMA may, as an example, determine that there is an insufficient Business Continuity and Disaster Recovery capability to withstand a ransomware attack – effectively the company's existence being at the mercy of one cyber incident perpetrated by a hacker with no means of recovery. A finding of this kind would recommend an immediate mitigation task before any other work is conducted.
- **Level of Effort:** Depending on the size of the organization, the RMA, like the Strategy can range from 1 to a multi-week level of effort. It is also typically combined with the Strategy and the Gap Analysis / Roadmap.
- **Owner:** The owner of the RMA deliverables is the CRO, CIO or CISO.
- **Alignment to business priorities and cyber infrastructure:** Solaris Consulting Group (SCG) will identify the organization's cyber risks aligned to the organization's business priorities and its cyber infrastructure, data directory / ownership / location, partner relationships, outsourcing and privacy impacts.
- **Key Elements:**
  - Analysis: High level view of the current state of cybersecurity risk across the business and the organization's priorities.
  - Identification and Categorization: The RMA identifies the cybersecurity risk arrayed by criteria so that risks can be understood by categories. This process yields better decision-making regarding level of urgency for mitigation, where the risk resides and the general mitigation approach. This data is further used by the gap analysis and roadmap.
- **The Solution Package:** The list of deliverables for this service offering includes:
  - Deliverable 1: Analysis to organize the cybersecurity risks by categories. The analysis is presented in a Word Document.
  - Deliverable 2: PowerPoint Executive Summary

## Features of RMA

- Identification of the cyber risks
- Threat profile
- Categorization to aid in decisions
- Urgency of mitigation

## Benefits of RMA

- Prioritization to focus the resources
- Prioritize to the business impacts
- Consistent to NIST CSF
- Informs the implementation