



Nombre del  
logotipo

## Project Title

# Organizational Situation Report

**Name of the organization:**

**Address of the organization:**

**Geolocation of the evaluated area:**

**Report date:**

**Prepared by:**

***Confidential, exclusive use of the client, etc.***



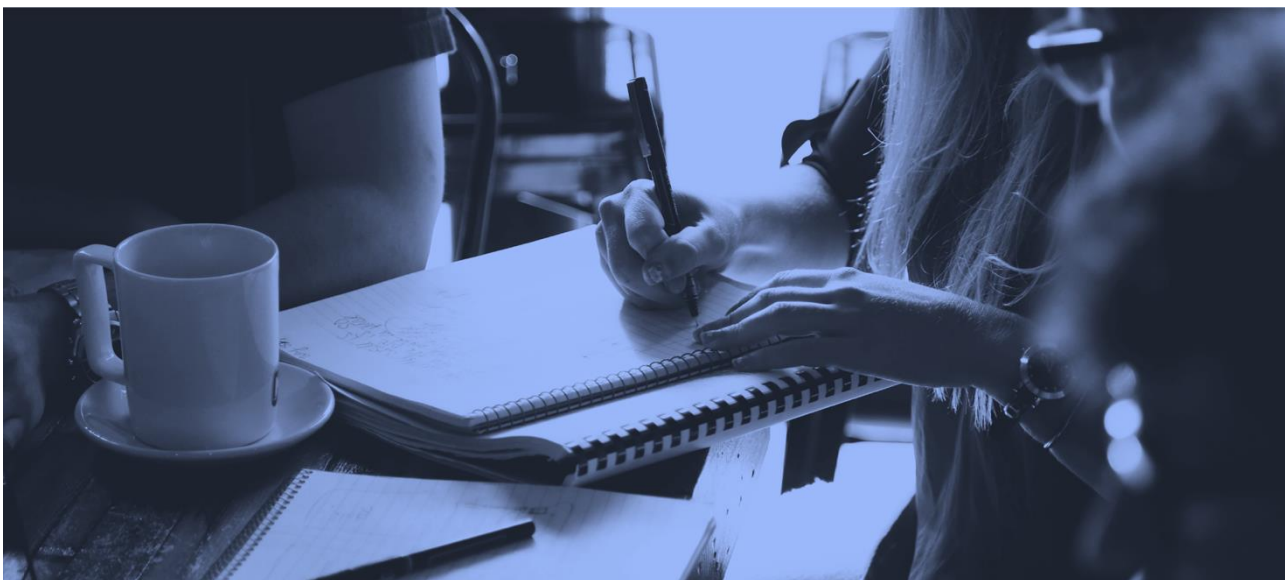
# CONTENTS

- Write Chapter Title (Level 1) ..... 1
  - Write Chapter Title (Level 2) ..... 2
    - Write Chapter Title (Level 3) ..... 3
- Write Chapter Title (Level 1) ..... 4
  - Write Chapter Title (Level 2) ..... 5
    - Write Chapter Title (Level 3)..... 6

## Executive Summary

The executive summary should provide a quick and effective overview of the key findings and recommendations from the report. Typically 1-2 pages, it is designed to give readers a concise view of the most important points:

- **General Overview of the Security Environment:** A summary of the current situation within the evaluated scope.
- **Key Findings:** Critical points requiring immediate attention, including a high-level summary of identified threats and vulnerabilities.
- **Key Actions to Implement:** A list of the most urgent actions the organization needs to undertake.
- **Next Steps:** Recommendations for future stages of the process, including reevaluations or implementation of new measures.



## Methodology

This section describes how information is collected, analyzed, and presented to evaluate the probability of risk in a country or region. It enables stakeholders to understand the foundation upon which assessments have been conducted and recommendations have been determined:

- **Purpose:** Explain that the objective of the methodology is to systematically and objectively evaluate the vulnerabilities and threats impacting security in a country or region over a specific period.  
**Scope:** Detail the scope of the analysis and the mechanisms used to assess vulnerabilities and identify and measure threats.  
**Evaluation Criteria:** Outline the specific criteria used to evaluate each area of vulnerability and threat.
- **Limitations and Exclusions:** List the assumptions, limitations, and exclusions considered during the preparation of the report. This section should be detailed to avoid misunderstandings or unrealistic expectations from the client.
- **References:** Cite any documents, standards, or guidelines used as references during the evaluation, such as the ASIS Security Risk Assessment Standard or other relevant frameworks.
- **Scoring Assignment:** Explain how scores are assigned to each evaluated criterion.
- **Score Averages:** Describe how average scores are calculated for each category (vulnerabilities and threats) and how these averages are used to determine an overall score representing the probability of risk in the country or region.
- **Probability Descriptors:** Explain how evaluation results are interpreted to classify the level of risk probability. This classification assists in prioritizing and categorizing the most critical areas requiring immediate intervention or continuous monitoring.
- **Contextualization:** Detail how results are contextualized within the broader landscape of the country. Include how the scores reflect the current situation and how they may evolve based on changes in the political, economic, or social environment.

## RISK IDENTIFICATION

This section of the report details the process of profile categorization.

- **Analysis of Vulnerabilities and Capabilities of the EPP:** Identification of internal and external vulnerabilities, as well as the organization's capacity to mitigate them.
- **Narrative on Identified Profiles:** Description of the categorization of executive profiles.
- **Criticality Analysis:** Evaluation of the potential severity of risks to profiles within the organization.

## RISK ANALYSIS

The report explains the process, moving from the specific to the general, used to analyze and prioritize executive profiles.

### Gap Analysis:

- Analysis of opportunities for improvement in the EPP.
- Organization's risk tolerance, determination of risk criteria, maximum threshold, and acceptable level of risk.
  - Identification of the organizational measures already implemented.
- Comparison of existing mitigations and their effectiveness against risk tolerance levels.

### Risk for Each Executive Profile

- Probability analysis:
- Vulnerability in the EPP.
- Threat to each executive profile.
- Criticality analysis by profile.

### Profile Evaluation

- Prioritization of profiles based on their risk level

### Identification of Profiles Above Tolerance Levels:

- Profiles that exceed acceptable levels for the organization and must be recorded for additional analysis.

## RISK ASSESSMENT

The situational report can convey qualitative results, though quantitative results tend to have greater impact when addressing managers and executives.

- **Probability of Organizational Risk:** A global assessment of the risk to the organization.
- **Risk Level by Executive Profiles:** A specific analysis of risks associated with various executive profiles within the organization.
- **Existing Mitigations:** Description of the strategies and protective measures currently in place for executive profiles.
- **Executive Profiles Managed with Existing Mitigations:** Identification of risks adequately managed by current strategies and measures.
- **Executive Profiles Requiring Additional Mitigations:** Risks that exceed the organization's tolerance and require additional strategies and measures.

## NECESSARY PROTECTION STRATEGIES AND MEASURES

This section details the options for managing and mitigating risks that are not at tolerable levels:

**Risk Avoidance:** Activities recommended to be avoided to completely eliminate the identified risk.

**Risk Transfer:** Use of insurance or other means to share the risk with third parties.

**Risk Optimization:**

- a) Reduction of the probability of occurrence through preparation and prevention measures to decrease the likelihood of the risk materializing.
- b) Mitigation of risks to the profile by reducing accessibility, exposure, predictability.
- c) Improving response in case the risk occurs, increasing capacity and response time.

**Risk Acceptance:** Informed decision to accept a risk due to the impossibility of mitigating it without incurring disproportionate costs.

**Cost-Benefit Analysis:** Evaluation of the proposed mitigations, considering their costs versus the benefits in terms of risk reduction. This connects to the budget and the Return on Executive Protection Investment (ROEPI) report.

## RESULTS AND CONCLUSIONS

This section consolidates the findings and recommendations from the SitRep:

**Conclusions and Recommendations from the SitRep:** Summary of the conclusions reached and recommendations to mitigate the identified risks.

**Alignment with the Organization's Risk Tolerance:** Explanation of how the recommendations align with the risk tolerance established by the organization.

**Steps for the Organization to Execute:** Specific recommendations on the actions the organization must carry out.

**Future Reevaluation Requirements:** Indication of when and how reevaluations should be conducted to ensure risks continue to be effectively managed.

## APPENDICES

The appendices include supplementary information that supports the content of the report and may include:

**Photos, Drawings, or Plans:** Relevant images that illustrate key points of the report.

**Crime Data and Statistics:** Quantitative information that supports the conclusions.

**Threat Log:** Characterization of capabilities and intent, as well as additional details about the identified threats.

**Backup Information:** Details about the custody of backups and the level of confidentiality.