# Security Assessments

## Introduction

For most businesses, creating a secure environment that is both efficient and cost effective is a mere dream. Putting in security measures to prevent a burglary, for example, can be simply a set of barriers that restrict operations and hinders the growth of the business. While paying lip service to the threat and investing in security measures that are ineffective is a waste of money.

The answer to this is a Security Risk Analysis.

In this short guide, we explain:

- What a security risk analysis is
- What the benefits are
- What's involved in an analysis
- What happens after a security risk analysis
- What the alternative options are

## What is a Security Risk Analysis used for?

The security risk analysis is the first step in the overall process of security management. It is a formal way for businesses (and individuals) to assess:

1. What can go wrong
2. What you can do about it
3. What to do when things do go wrong

*For example, all doors need locks, but a security risk analysis will determine if crime is such a threat that those doors need to be alarmed or further strengthened with grilles/gates.*

The process is recurring and should be repeated regularly. In fact, as the process is repeated, a more accurate picture emerges of the security risk.

## What are the benefits of a Security Risk Analysis?

One of the key requirements for the success of the Security Risk Analysis is the directive from senior management. If conducted with the collaboration of line managers (something that will only succeed with the backing of senior management), then the security analysis will:

- ✓ Highlight areas that need greater (or lesser) security controls.
- ✓ Help build awareness amongst employees of the potential strengths and weaknesses of the security measures.
- ✓ Help build a business case for the development and justification of cost-effective countermeasures to protect the business and employees.
- ✓ Help create buy-in from employees to the security measures and overall security plan.

equilibrium risk
security & risk management

# What's involved in a Security Risk Analysis?

**Identify the Assets**
- Identify the assets that need protecting
- Characterise the context in which they exist

**Determine the Threats**
- Threats - source of potential harm
- Identify the potential of the threats

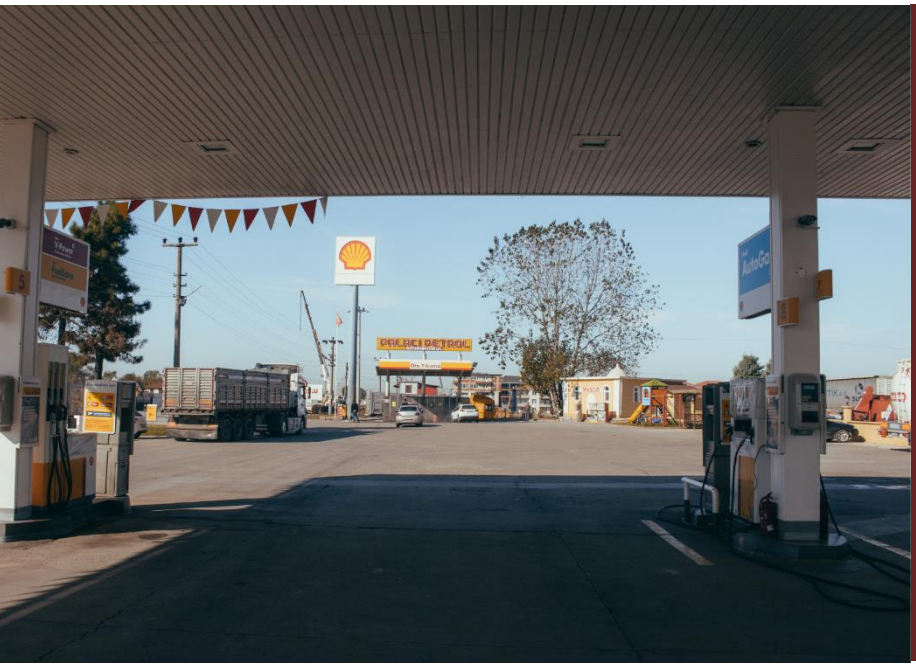
**Assess the Probability**
- Probability - the likelihood that threat will occur
- Estimate the probability of each threat

**Gauge the Impact**
- Impact - the damage (direct and indirect) that would occur if the threat materialised.
- Determine the potential impact to the asset if the threat occurs.

**Plot the Risk Value**
- Plot impact and likelihood on a graph to determine a level of "raw" risk

**Establish the Vulnerability**
- Vulnerability - a weakness or a flaw in a security system or any business process that could conceivably be exploited by a threat.

**Prioritise the Risk**
- Risk - the potential for loss, considering the likelihood, impact and vulnerabilities.
- Measure the "raw" risk against vulnerability or controllability to determine protection priorities.



Most petrol stations have standard baseline security measures in place (CCTV, safes, duress buttons, locks, intrusion detection etc).

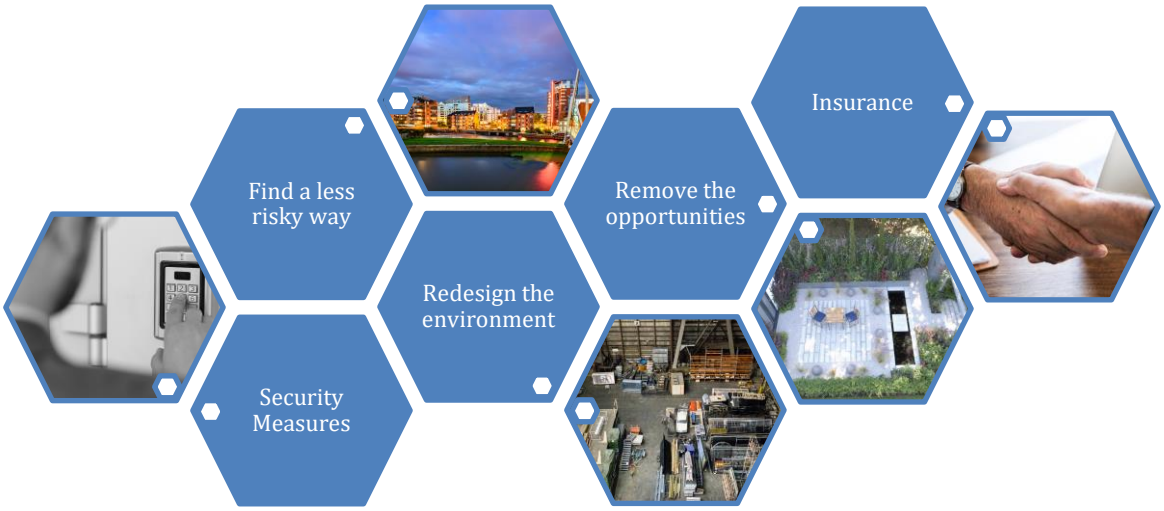
But where the risk analysis indicates an elevated risk of robbery there will be a need for enhanced measures during hours of darkness, such as shop lock-down and service through a bullet-resistant hatch or pay-at-the-pump.

Equilibrium Risk Ltd
3M Buckley Innovation Centre, Firth Street, Huddersfield, West Yorks. HD1 3BD
enquiries@equilibriumrisk.com | www.equilibriumrisk.com | T: 01484 505321
Registered in England and Wales, Company No. 8367278

## What happens after a Security Risk Analysis?

Having analysed, and then prioritised your risks, they should then be mitigated. This can be achieved by a variety of strategies, including:

- ✓ The application of security measures.
- ✓ Redesign of the environment to make crime riskier to the perpetrator.
- ✓ Finding a less risky way to undertake a business activity.
- ✓ Removing the opportunities and inherent business vulnerabilities.
- ✓ Insurance.




## What other alternative options are there?

Although a Security Risk Analysis finds the most efficient, cost-effective way of protecting your business, you do have other options:

- ➢ **Baseline Security** – Putting in place baseline security measures (access control systems, barriers, surveillance, guards, procedures etc.) in the belief that this is a sufficient catch-all solution capable of addressing most types of misconduct and crime. This is an instinctive approach to security and is widely practiced.
- ➢ **Packaged Security** – This is another very common approach to commercial security in which a company determines by policy what kinds of measures are appropriate according to the facility type. This may also include security measures that are mandatory according to company policy, by code or contractual undertaking, or by law.
- ➢ **Security Vulnerability Analysis** – A process in which a business is physically examined to identify vulnerabilities in protection that could provide opportunities for crime. For this to be effective there must be an understanding of prevalent local crimes.