PURPOSE AND SCOPE

The purpose of conducting Site Security Risk Assessments is to provide an organization with a comprehensive view of the risks that their operational sites face, and the current and potential mitigating measures to manage these risks.

A Site Security Risk Assessment is necessary for organizations to ensure that the current or planned level of security is aligned with the accepted level of risk, cost, and compliance with internal and external requirements.

OBJECTIVES

A Risk Assessment should give the organization:

- [ ] A prioritized list of the relevant threats.
- [ ] The nature of the threats, such as modus operandi and the vulnerabilities that can be exploited
- [ ] The potential impact and likelihood, expressed as a threat level
- [ ] A risk level based on the threat level, adjusted for the vulnerabilities
- [ ] The effect of current mitigation measures already implemented
- [ ] The level of compliance against requirements (internal and external), based on elements such as the general risk level, business criticality of the site, products and services produced or delivered, laws and regulations.
- [ ] Relevant triggers (future changes or developments i.e. incidents, intelligence or information) that could indicate a change in the threat landscape and/or level of risk
- [ ] The need for either additional or fewer measures.
- [ ] The financial implications of everything above
- [ ] Responsibilities and required ongoing activities

SCOPE

At beginning of the process it is crucial to establish the context in which the Risk Assessment is being conducted. This includes:

- Identifying pillars of the organization's business strategy
- Conducting a stakeholder analysis
- Scrutinizing the organization's security policy

The structure of a Risk Assessment should include the following sections:

Situational Analysis

A thorough investigation of relevant external and internal site factors to determine the relevant threats

- External elements
  - History
  - Attractiveness of the site
  - Context
  - Intelligence
  - Intent and capability of the adversaries
  - Compliance
- Internal elements
  - Operational patterns
  - Staff composition
  - Business criticality / business continuity requirements
  - Previous incidents
  - Company values and leadership style

Conclusion

Summary of the key findings from the situational analysis that addresses the objectives of a Risk Assessment, and includes

- Financial analysis
- Recommendations

Ongoing Management

Details of stakeholder responsibilities and any ongoing requirements and tasks that should be completed based on the findings of this Risk Assessment.

Threat and Measure Catalog

Details of the identified threats and their nature, threat levels, and of the implemented and potential mitigating measures and their effects.