ESTABLISHING CONTEXT: SECURITY POLICY REVIEW

Your organization's security policy represents the core elements and values of the security program, which are important to keep in mind when creating a Risk Assessment. To determine the scope of the Assessment, there are four key elements from the overall security policy that should be considered:

- 🟢 What the organization wants security to do – the overall objective
- 🟠 What the organization is protecting
- 🔴 What it is being protected from
- 🔵 How it is being protected

🟢 PART 1: THE OVERALL OBJECTIVE

What is the overall objective of the security policy? There should be a specifically-stated goal, such as fostering a safe work enviroment. This will help you identify the expected level of risk acceptance, which will guide the type and amount of mitigation measures suggested in the Risk Assessment.

🟠 PART 2: WHAT NEEDS TO BE PROTECTED?

What is your organization protecting? This will typically include people and assets, but information, processes, integrity and/or reputation may also be specifically mentioned. Knowing what needs to be protected will help determine the potential threats that should be included in your Risk Assessment and who you may need to liaise with, both internally and externally.

PART 3: WHAT ARE YOU PROTECTING FROM?

Does your organization's security policy make note of specific threats or characteristics of the environments it operates in? These aspects are important to include in the Risk Assessment.

Threat / Characteristic:

Threat / Characteristic:

Threat / Characteristic:

Threat / Characteristic:

PART 4: HOW ARE YOU PROTECTING?

What are the overall governance processes of the security program? Who has what responsibilities, and where does decision-making power lie? This understanding will also come from and work into the Stakeholder Analysis.

Also relevant here are any standards mentioned in the policy that should be included in the Risk Assessment. This may include risk categorization of sites, minimum requirements, or non-security requirements such as industry standards or legislation.