* A high-level summary of the **audit scope** is provided (4-6 sentences or bullet points)

The idea is to present a formal cybersecurity strategy which follows the best practices and standards to protect the whole IT infrastructure of the company given the current mediocre state of affairs respect to a vital issue for businesses today.

* A high-level summary of the **audit goals** is provided (4-6 sentences or bullet points)

It is mean to demostrate the capabilities and readiness of the IT department of the company through a complete audit of the cybersecurity posture of the company to the stakeholders.

* **Critical findings** are listed and explained

It was found that the company IT deparment is not implementing neither following industry best practices and standards which ultimately can cost the company reputational and financial damage.

* Other **findings** are listed and explained

Perhaps the most shocking is that there is not any system in place to track the company assets.

* The **summary/recommendations** clearly and concisely synthesize the the most important information from the audit scope, goals, critical and other findings (5-10 sentences)

Nowdays, the internet offers great advantages for global outreaching, however a company that it is not putting much emphasis in its IT infrastructure is exposed to the numerous risks that plague the internet. Fortunately, there has been already great efforts to create frameworks and standards to deal or at least mitigate these issues. Furthermore, at the present virtually every country in the world demand by law some more strict than others that companies must adhere to these standards and practices to ensure the protections of business and customers data alike which may be punishable by law for not following them as any other laws that govern other spectrums.