

spector

# Cyber Security Gap Analysis

The first step to understand  
and address your risk.

# Why perform a Cyber Security Gap Analysis?

Our Gap Analysis helps you to benchmark your current Cyber Security posture and identify your organisation's critical IT risks. It allows you to focus your attention and budget on the highest priority risks, while improving overall Cyber Security maturity levels.

---

**“A Cyber Security Gap Analysis is invaluable in outlining the differences between the current and ideal state of IT security in your business.”**



# How it Works

## 1 - Start with Strategy

---

The logical first step is to define your Cyber Security strategy and desired outcomes. Whether this is achieving a standard such as ISO 27001, meeting Regulatory and Audit Requirements, or simply improving your overall Cyber Security posture. This strategy discussion sets the stage for the Frameworks and Controls to help guide you through your Cyber Security journey.



Start with Strategy

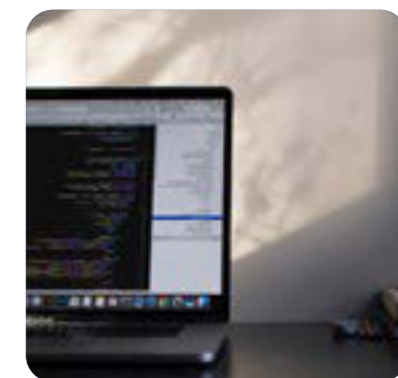
---

---

**“The Spector Cyber Security Gap Analysis is the first step in identifying weaknesses in your IT setup and staying ahead of the cyber crime.”**

Perform the Gap Analysis

---



Identify the Key Risks

---

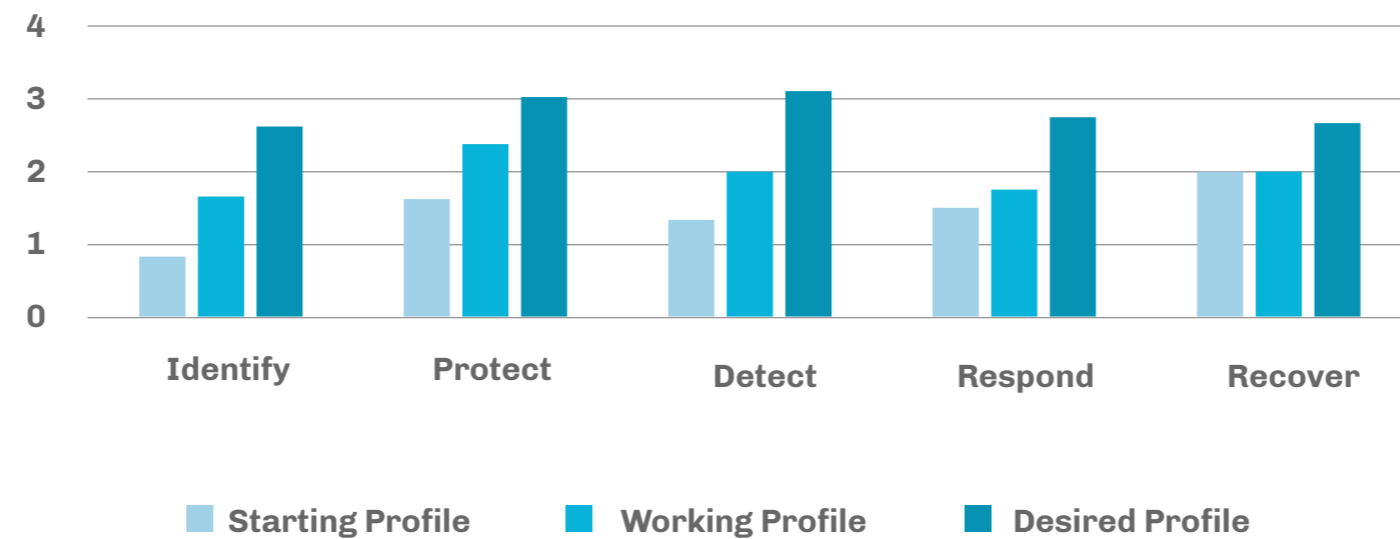


# How it Works

## 2 - Perform the Gap Analysis

Spector typically leverages the NIST Cybersecurity Framework in order to provide structure for our work. We assess your organisation's current and target Cyber Security profiles. The difference between these profiles provides the GAP analysis, and defines risks over 5 key functional areas: Identify, Protect, Detect, Respond and Recover.

**NIST Cyber Security Framework - Assessment Scoring**



# How it Works

## 3 - Identify the Key Risks

---

Once we have a clear picture of the gaps, we can then assess the associated risks. First, we identify the inherent risk and the organisational risk appetite. The knowledge obtained thus far will inform us of the key vulnerabilities found in your current structure.

This process then indicates which risks should be dealt with first and allows us to create an Action Plan based on your priorities. The goal is to protect your business from these imminent risks, before moving on to address more complex matters.



# Outcomes

We understand that there are often different levels at which this information is targeted in an organisation. So, it is with this in mind that we provide a version of these findings that is appropriate for both the profiles in charge of making decisions, and those responsible for analysing and executing the tasks. All delivered in plain English and terms that your peers will understand. Our delivery includes:

**1**

**Complete Report:** containing a detailed analysis of your security posture over 23 key areas, with all specific benchmarks from our findings. This level of detail provides full coverage of your business's tech infrastructure.

**2**


**Board Report:** a summarised version of our findings in a report and slide format for consumption by the Board and Senior management, highlighting the central issues that they need to know.

**3**

**Action Plan:** we also identify projects and measures to help you attain your goals. Learning about your issues is vital, but identifying the right priorities and solutions is what will truly benefit your business.





 +353 1 664 4190

 [info@spectator.ie](mailto:info@spectator.ie)