PRIFYSGOL BANGOR UNIVERSITY

Author: Will Hughes
Supervisor: Dr. Saad Mansoor

Information Security – Gap Analysis

Introduction

Information security is **critical** for the organisations of today. A report published by IBM in 2020 found that the average data breach has a **total cost of $3.86m (£2.77m)** with **80% of breaches involving identifiable customer information** and **53% of attacks being identified as financially motivated[1].** With the correct tools and analysis, data breaches are easily avoidable. In the field of Information Security, Organisations will use a Gap Analysis and risk assessment(s) to help identify and protect organisations from such data breaches.

What is a Gap Analysis?

A Gap Analysis is widely used in many fields, it is discovering the "gap" between an organisation's current performance and targeted performance. In the context of Information Security, a Gap Analysis would help identify what steps an organisation would need to meet in order to achieve recognised international standards; such as ISO 27001.

Figure 1

Gap Analysis Methodology

As shown in Figure 2 – The standard to be met is identified, which is then used by the evaluator using a checklist/audit to assess the actual performance of the organisation and how they compare to the chosen standard. This then allows for a gap analysis report to be generated.

As part of my research, I will be conducting a Gap Analysis on Bangor University's IT Services to identify their current performance and highlight any steps that need to be taken to achieve their chosen information security standards.

A report will then be developed which clearly conveys my findings from the analysis.

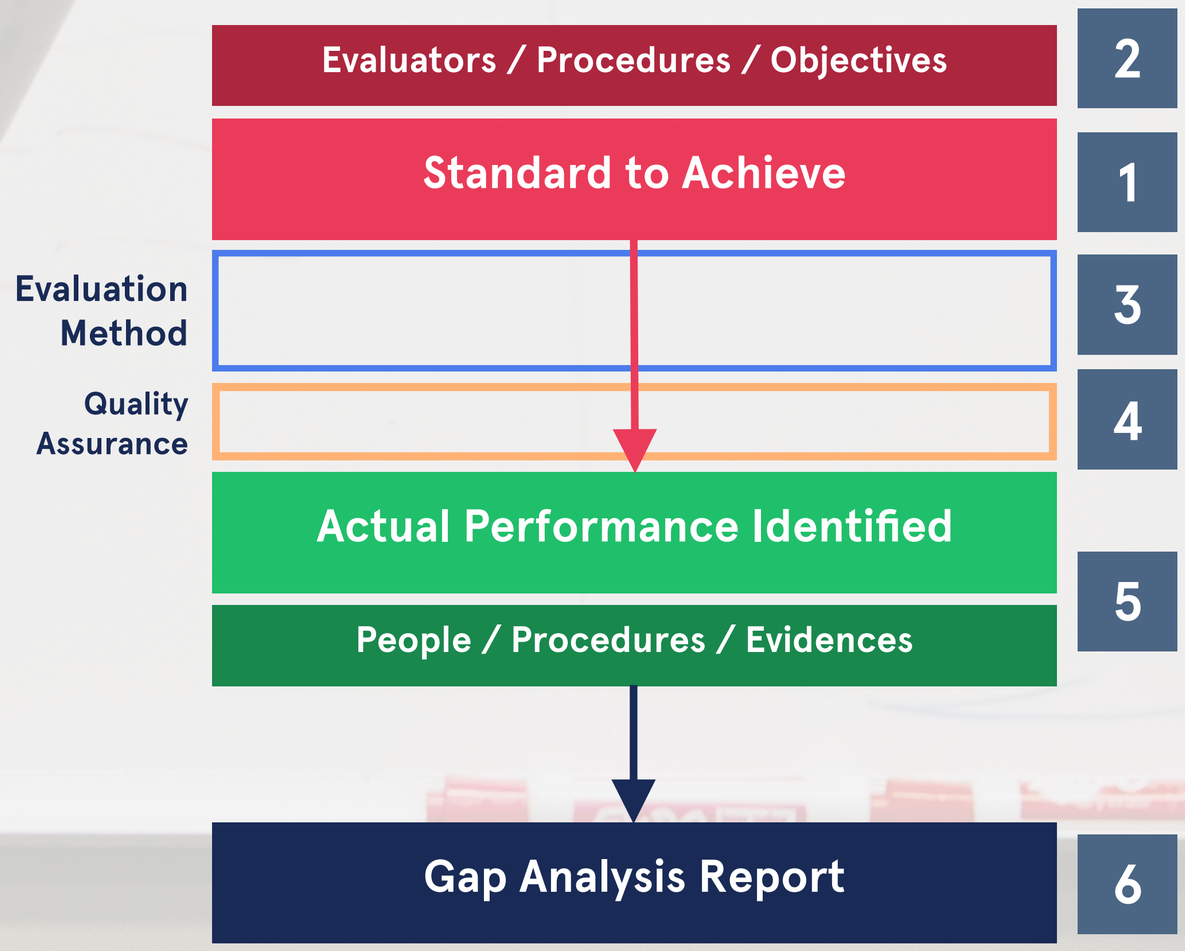

Figure 2

[1] IBM Corporation, 2020. Cost of a Data Breach 2020. IBM Security, p.5.