# Gap Analysis Template for UK Cyber Essentials Framework

Assessment and Planning for Cyber Security Compliance

## Introduction

The UK Cyber Essentials framework provides a set of security measures designed to protect organisations against common cyber threats. This gap analysis template assists businesses in identifying areas where their current security practices do not meet the requirements of the framework, helping them develop a plan to address these gaps and achieve certification.

## Executive Summary

This section should provide an overview of the gap analysis's purpose and scope, as well as a summary of the findings. It should highlight key areas of non-compliance and propose high-level recommendations for achieving Cyber Essentials certification.

## Background

### Company Overview

Please briefly describe the company, including its size, industry, and key stakeholders.

### Cyber Essentials Framework

Outline the key components and objectives of the Cyber Essentials framework.

### Current Security Posture

Summarise the organisation's current cybersecurity measures and practices.

## Gap Analysis Methodology

### Assessment Approach

Describe the approach to assessing compliance with the Cyber Essentials framework, including the tools and techniques used.

### Data Collection

Detail the sources of information used in the assessment, such as interviews, document reviews, and technical testing.

### Analysis Process

Explain how the collected data was analysed to identify gaps and areas of non-compliance.

## Findings

### Summary of Compliance

Provide a summary of the organisation's compliance status with each requirement of the Cyber Essentials framework.

### Identified Gaps

For each requirement, list the specific areas where the organisation is not compliant. Use the following format for each requirement:

Requirement 1: Boundary Firewalls and Internet Gateways

- Current Status: Brief description of the organisation's current practices.
- Gap: Detailed description of non-compliance areas.
- Impact: Explanation of the potential risks associated with the gaps.
- Recommendation: Suggested actions to achieve compliance.

Requirement 2: Secure Configuration

- Current Status: Brief description of the organisation's current practices.
- Gap: Detailed description of non-compliance areas.
- Impact: Explanation of the potential risks associated with the gaps.
- Recommendation: Suggested actions to achieve compliance.

Requirement 3: Access Control

- Current Status: Brief description of the organisation's current practices.
- Gap: Detailed description of non-compliance areas.
- Impact: Explanation of the potential risks associated with the gaps.
- Recommendation: Suggested actions to achieve compliance.

Requirement 4: Malware Protection

- Current Status: Brief description of the organisation's current practices.
- Gap: Detailed description of non-compliance areas.

- Impact: Explanation of the potential risks associated with the gaps.
- Recommendation: Suggested actions to achieve compliance.

Requirement 5: Patch Management

- Current Status: Brief description of the organisation's current practices.
- Gap: Detailed description of non-compliance areas.
- Impact: Explanation of the potential risks associated with the gaps.
- Recommendation: Suggested actions to achieve compliance.

# Recommendations

## Priority Actions

Identify and prioritise the most critical actions needed to address the gaps and achieve compliance.

## Implementation Plan

Provide a detailed plan for implementing the recommended actions, including timelines, responsible parties, and required resources.

## Monitoring and Review

Outline a process for ongoing monitoring and review to ensure continued compliance with the Cyber Essentials framework.

# Conclusion

Summarise the key findings of the gap analysis and reiterate the importance of achieving Cyber Essentials certification. Emphasise the benefits of enhanced cybersecurity for the organisation.

# Appendices

## Appendix A: Detailed Assessment Results

Include detailed assessment results for each requirement, providing specific evidence and observations to support the findings.

## Appendix B: Implementation Resources

List resources, such as external consultants, tools, and training programs, that can assist with implementing the recommended actions.

### Appendix C: Glossary

Provide definitions of key terms used in the gap analysis report.

## References

List any sources of information, standards, or guidelines referenced in the gap analysis.

This template is a comprehensive guide to conducting a gap analysis for the UK Cyber Essentials framework. By following the structure and methodology outlined, organisations can systematically identify and address areas of non-compliance, ultimately achieving certification and strengthening their cybersecurity posture.