

Blue Team Level 1 Certification
(Standard)

6 Topics | 1 Quiz

✓ Management Principles

4 Topics | 1 Quiz

✓ Section Introduction, Management Principles

✓ Risk

✓ Policies and Procedures

✓ Compliance & Frameworks

📄 Activity) End of Section Review, Management Principles

PHISHING ANALYSIS DOMAIN

✓ PA1) Introduction to Emails and Phishing

7 Topics | 1 Quiz

✓ PA2) Types of Phishing Emails

10 Topics | 2 Quizzes

✓ PA3) Tactics and Techniques Used

12 Topics | 2 Quizzes

✓ PA4) Investigating a Phishing Email

8 Topics | 2 Quizzes

○ PA5) Analysing URLs, Attachments, and Artifacts

8 Topics | 1 Quiz

○ PA6) Taking Defensive Actions

12 Topics | 1 Quiz

○ PA7) Report Writing

7 Topics | 1 Quiz

○ PA8) Phishing Response Challenge

3 Topics | 1 Quiz

THREAT INTELLIGENCE DOMAIN

○ TI1) Introduction to Threat Intelligence

7 Topics

Section Introduction, Management Principles

Blue Team Level 1 Certification (Standard) > Management Principles > Section Introduction, Mana...

COMPLETE

Security Fundamentals SECTION INTRODUCTION



This section of the Security Fundamentals domain will cover core cybersecurity and management principles such as risk, compliance, and policies and procedures. As cybersecurity is all about reducing risk to the business, it is important to understand what risk is, and how we can address it. Compliance ensures that organizations meet a minimum standard of security to comply with legal and regulatory requirements and understanding the importance of policies and procedures to help maintain security within an organization.

LEARNING OBJECTIVES

By the end of this section you will have achieved the following objectives:

- Understand and explain what risk is, in a business context.
- Understand what policies and procedures are, and why they're so important in information security.
- Understand what compliance is, and some of the frameworks that organizations must abide by.

[< Previous Lesson](#)[Back to Lesson](#)[Next Topic >](#)[Privacy & Cookies Policy](#)