IT Nation Certify   
Cybersecurity Fundamentals (CCFX)

Certification Syllabus

# How to Use This Document

Check out the information below to see our recommendations for using this document to help meet your goals.

## Planning

We highly recommend using this document to plan your progress in your certification. While it can be tempting to cram all of the content in one day, if you’re interested in sincerely acquiring the knowledge, the best technique is to create a plan for completion.

To do this:

1. Establish your due date.
   1. Decide when you’d like to be done with the certification.
2. Determine the number of days you can dedicate to learning the material.
   1. Evaluate your calendar and count the number of days between now and your deadline. Eliminate vacation, busy, and otherwise off-limit days.
3. Use the Estimated Time to Complete (ETC; under the Certification Structure in this document) for each Lesson to block time on each of the days on your calendar. For best results:
   1. Be sure to schedule an extra 10 minutes at the start of each of your blocks. Use the time to review previous concepts before jumping into the new material.
   2. Add 1-3 extra time blocks before the due date that are just for reviewing the materials and retaking any practice exams. You can also use this time to reach out to the course expert with any lingering questions, or post to the forums to reinforce your learning.
4. Keep those appointments to finish the courses.
   1. Reschedule as necessary but be careful not to set yourself up for cramming at the end.
5. Take the certification and meet your goal!

## Portfolio & Performance Reviews

Use the Course Objectives to identify the specific knowledge and skills you have acquired by completing this certification.

Remembering everything you did in one year is hard. Do your future self a favor:

* Save this document in a folder (along with other pamphlets, brochures, screenshots, emails, etc.) from professional development opportunities you complete throughout the year. This can help you track and plan your career growth while making it easier to prepare for career-related conversations your supervisor.

# Certification Description

The Cybersecurity Fundamentals Certification includes on-demand courses with MSP-specific cybersecurity training to protect your own practice, gain confidence in your ability to provide cybersecurity services to your clients, and drive security sales growth. The delivery of these self-paced courses includes lectures, activities, and practice exams.

The Cybersecurity Fundamentals Certification includes the following coursework:

1. Cybersecurity Fundamentals
2. Choose One:
   1. Cybersecurity Fundamentals for Sales and Owners
   2. Cybersecurity Fundamentals for Engineers
3. Cybersecurity Fundamentals Certification Exam (Sales/Owners or Engineers)

# Course Objectives

After successfully completing each course, you will be able to:

## Cybersecurity Fundamentals

1. Identify the different phases of the Security Journey to maturity as they apply to the SECURE MSP+ practice, where the MSP fits into each phase and key areas for improvement.
2. Explain why awareness, behavior modification, discussion, and culture transformation support a SECURE MSP+ practice.
3. Recognize examples of governance, what it is, and the role it plays in risk management.
4. Describe what a Framework is and identify which ones are most used on both a global and national basis, how they complement or intersect with each other, and why Frameworks are important.

## Cybersecurity Fundamentals for Sales and Owners

1. Describe cyber technology.
2. Define risk management and security assessments.
3. Identify key areas of the sales roadmap.
4. Explain the benefits of providing live security awareness training.
5. Elaborate on business outcomes tied to cybersecurity.

## Cybersecurity Fundamentals for Engineers

1. Describe governance.
2. Explain implementation groups.
3. Elaborate on secure onboarding and what it entails.
4. Define malware attacks.
5. Identify key areas in incident response planning.

# Certification Structure

The Cybersecurity Fundamentals certification is completely online, on-demand, and self-paced.  You’ll be introduced to some fundamental topics to start, then take a deeper dive into more intermediate and advanced topics in the Engineers and Sales courses that follow. Below is a summary of the certification topics, broken down by course and lesson, as well as the estimated time to complete (ETC):

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Course** | | **Lesson** | | **Topics** | | **ETC** | |
| **Cybersecurity Fundamentals** | | Introduction to Cybersecurity | | 1. Introducing Cybersecurity 2. Covering Common Vocabulary and Acronyms 3. Understanding Cybersecurity Culture 4. Discovering Cybersecurity Models | | 30 min. | |
| The Security Journey | | 1. Exploring the Security Journey 2. Completing the Security Journey Assessment | | 30 min. | |
| Governance, Risk, and Compliance | | 1. Introduction to the GRC 2. Examining Governance 3. Reviewing Risk 4. Identifying Where You Are in the Security Journey | | 30 min. | |
| The Three Pillars of Cybersecurity | | 1. Introducing the Three Pillars of Cybersecurity 2. Examining the People Pillar of Cybersecurity 3. Exploring the Process Pillar of Cybersecurity 4. Supporting with the Technology Pillar | | 30 min. | |
| Cybersecurity Controls | | 1. Introducing the Cybersecurity Controls 2. Covering the Controls and Layers of Security | | 30 min. | |
| Cybersecurity Frameworks | | 1. Establishing Cybersecurity Frameworks 2. Explaining the NIST Framework | | 30 min. | |
|  | |  | |  | |  | |
|  | |  | |  | |  | |

**Role-Based Courses (Choose One):**

|  |  |  |  |
| --- | --- | --- | --- |
| **Course** | **Lesson** | **Topics** | **ETC** |
| **Cybersecurity Fundamentals**  **for Sales and Owners** | Cyber Technology | 1. Understanding the Cybersecurity Stack 2. How Do We Build Our Stack? | 30 min. |
| Risk Management and Security Assessments | 1. The Security Assessment Process | 15 min. |
| Sales Roadmap | 1. Qualifying Questions 2. Risk and Security Awareness Presentations 3. Objection Handling 4. Call to Action Samples | 60 min. |
| Live Security Awareness Training | 1. Live Security Awareness Training | 15 min. |
| Business Outcomes | 1. Business Outcomes | 5 min. |

|  |  |  |  |
| --- | --- | --- | --- |
| **Course** | **Lesson** | **Topics** | **ETC** |
| **Cybersecurity Fundamentals**  **for Engineers** | Governance | 1. Governance | 5 min. |
| Implementation Groups | 1. Implementation Group 1 2. Implementation Group 2 3. Implementation Group 3 | 45 min. |
| Secure Onboarding | 1. A Secure Onboarding Process 2. Cheat Sheet | 40 min. |
| Malware Attack Concepts | 1. Malware Attack Concepts | 20 min. |
| Incident Response Planning | 1. Incident Response Planning Before, During and After an Incident | 20 min. |

Exams

Each course in the certification has one practice exam. There is one final certification exam for each role-based track; one for Sales/Owners and a different exam for Engineers.

## Certification Exam

The certification exam is cumulative. Exams can be found under [My Transcript](https://university.connectwise.com/University/CourseWork.aspx#cw) on the University. Here are the requirements:

* You must complete all coursework before the Exam is unlocked.
* The exam consists of 40 multiple choice questions.
* You will have one (1) hour to complete the exam.
* You must score at least 80% to pass the final exams.

## Practice Exams

Each of the Cybersecurity Fundamentals courses includes a practice exam with questions from the certification exam. These practice exams require a score of 80% or higher to progress in the certification.