30-Day Study Plan for the ISC² Certified in Cybersecurity (CC) Exam

📌 How to Use This Study Plan

- **Daily Commitment:** Spend **1-2 hours per day** studying.
- **Weekly Review:** At the end of each week, review key concepts and practice questions.
- **Practice Tests:** Take full-length practice exams to assess your readiness.
- **Focus on Weak Areas:** Spend extra time on challenging topics.
- **Stay Consistent:** Avoid cramming—stick to the schedule!

🗓️ Week 1: Foundations of Cybersecurity & Security Principles

Day 1: Understanding Cybersecurity & Information Assurance

✅ Introduction to cybersecurity concepts.
✅ Importance of **Confidentiality, Integrity, and Availability (CIA Triad)**.
✅ Real-world examples of cybersecurity risks.
📖 **Review:** Chapter 1, Module 1 (Security Concepts).

Day 2: Authentication & Access Control

✅ Learn about **authentication factors (MFA, biometrics, passwords)**.
✅ Understand **Non-Repudiation & Privacy** in cybersecurity.
📖 **Review:** Chapter 1, Module 1.

Day 3: Risk Management Fundamentals

✅ Identify security risks using **risk assessment frameworks (NIST, ISO 27005)**.

✅ Risk prioritization and treatment strategies.

📖 **Review:** Chapter 1, Module 2.

Day 4: Security Controls (Technical, Administrative, and Physical)

✅ Difference between **Preventive, Detective, and Corrective Controls**.

✅ Learn about **Firewalls, IDS, Encryption, and Security Awareness Training**.

📖 **Review:** Chapter 1, Module 3.

Day 5: Governance & Compliance

✅ Understand the role of **Policies, Procedures, and Standards**.

✅ Learn about key cybersecurity regulations (**GDPR, HIPAA, ISO 27001, PCI DSS**).

📖 **Review:** Chapter 1, Module 4.

Day 6: ISC² Code of Ethics

✅ Review the **Four Canons of the ISC² Code of Ethics**.

✅ Learn ethical responsibilities of cybersecurity professionals.

📖 **Review:** Chapter 1, Module 5.

Day 7: Weekly Review & Practice Questions

✅ Go over key topics from Week 1.

✅ Attempt full length **practice test covering Security Principles**.

🗓️ Week 2: Business Continuity, Disaster Recovery & Incident Response

Day 8: Introduction to Business Continuity & Incident Response

✅ Learn about **Business Continuity Planning (BCP) & Disaster Recovery Planning (DRP)**.

✅ Differences between **BCP and DRP**.

📖 **Review:** Chapter 2, Module 1.

Day 9: Understanding Incident Response (IR) Phases

✅ Learn the **NIST Incident Response Framework** (**PDCERP** – Preparation, Detection, Containment, Eradication, Recovery, Post-Incident Review).

📖 **Review:** Chapter 2, Module 1.

Day 10: Business Continuity Components

✅ Learn about **Risk Assessment, Business Impact Analysis (BIA), and Recovery Strategies**.

📖 **Review:** Chapter 2, Module 2.

Day 11: Disaster Recovery Strategies

✅ Recovery Time Objective (RTO) vs. Recovery Point Objective (RPO).

✅ Hot, Warm, and Cold Backup Sites.

📖 **Review:** Chapter 2, Module 3.

Day 12: Incident Response in Action

✅ Learn how to detect, respond, and mitigate real-world security incidents.

📖 **Review:** Chapter 2, Module 1.

Day 13: Security Drills & Testing

✅ Conduct a **tabletop exercise** for an incident response scenario.

📖 **Review:** Chapter 2, Modules 1 & 2.

Day 14: Weekly Review & Practice Questions

✅ Attempt **full length practice test** from on BCP, DRP, and IR.

🗓️ Week 3: Access Control & Network Security

Day 15: Access Control Fundamentals

✅ Understand **Logical vs. Physical Access Control**.

✅ Learn about **Role-Based Access Control (RBAC), Discretionary Access Control (DAC), and Mandatory Access Control (MAC)**.

📖 **Review:** Chapter 3, Module 1.

Day 16: Authentication Mechanisms

✅ Learn about **Multi-Factor Authentication (MFA)** and **Principle of Least Privilege (PoLP)**.

📖 **Review:** Chapter 3, Module 1.

Day 17: Physical Security Controls

✅ Review **Badge Systems, CCTV, Security Guards, and Environmental Controls**.

📖 **Review:** Chapter 3, Module 2.

Day 18: Network Security Basics

✅ Learn about **OSI Model (7 Layers) and TCP/IP Model (4 Layers)**.

📖 **Review:** Chapter 4, Module 1.

Day 19: Cyber Threats & Attacks

✅ Study **DDoS, Malware, Phishing, Man-in-the-Middle (MITM) attacks**.

📖 **Review:** Chapter 4, Module 2.

Day 20: Network Security Infrastructure

✅ Learn about **Firewalls, IDS, IPS, VPNs, and Network Segmentation (DMZ, VLANs)**.

📖 **Review:** Chapter 4, Module 3.

Day 21: Weekly Review & Practice Questions

✅ Attempt **full length** practice test from Access Control & Network Security.

🗓️ Week 4: Security Operations & Final Exam Prep

Day 22: Data Security & Encryption

✅ Learn about **Symmetric vs. Asymmetric Encryption (AES, RSA, Hashing)**.

📖 **Review:** Chapter 5, Module 1.

Day 23: System Hardening & Patch Management

✅ Review **Configuration Management, Patching, and Secure Baselines**.

📖 **Review:** Chapter 5, Module 2.

Day 24: Best Practice Security Policies

✅ Learn about **Password Policies, Acceptable Use Policies (AUP), BYOD Policies**.

📖 **Review:** Chapter 5, Module 3.

Day 25: Security Awareness Training & Social Engineering

✅ Understand **Phishing, Social Engineering, and Security Awareness Training**.

📖 **Review:** Chapter 5, Module 4.

Day 26: Final Review of Key Concepts

✅ Go over **high-priority topics** (BCP, IR, Encryption, Network Security).

✅ Memorize key **acronyms and mnemonics** for the exam.

Day 27: Full-Length Practice Test (1)

✅ Take a **100-question practice exam**.

✅ Review incorrect answers to identify weak areas.

Day 28: Targeted Review & Weak Area Focus

✅ Focus on **topics where you scored low on the practice test**.

✅ Review **Security Controls, Threats, and Incident Response**.

Day 29: Full-Length Practice Test (2)

✅ Take another **100-question practice exam**.

✅ Aim for **80% or higher** to ensure exam readiness.

Day 30: Final Quick Review & Exam Readiness Check

✅ Revise your **notes, flashcards, and key concepts**.
✅ Get a **good night's sleep** before the exam!

🎯 Study Plan Summary

✔ **Daily Learning:** 1-2 hours per day on specific topics.
✔ **Weekly Reviews:** Practice questions at the end of each week.
✔ **Hands-On Exercises:** Risk assessment, incident response drills, and system hardening.
✔ **Final Week Focus:** Full-length practice exams and weak area improvement.

📌 **Final Tip:** Stay **consistent and confident!** You're now ready for the ISC² Certified in Cybersecurity (CC) Exam. 🚀