COURSE CONTENT

www.ciccsglobal.com
info@ciccsglobal.com

CCCA CURRICULUM
CANDIDATES EXAM GUIDE

The Chartered Compliance and Cyber Analyst (CCCA) professional exam consist of three (3) levels and is written twice every year, which is, last week of January and July of every year for members who have discharged all their financial obligations to the Institute .The CCCA exams consist of fourteen (14) papers and there shall be no exemption in level three (3). All level one and two exams shall consist of twenty (20) objective questions and four (4) subjective questions. All part three exams shall consist of five (5) subjective questions

LEVEL I

1. CYBER SECURITY OPERATIONS **(CC 1)**
2. ENTERPRISE LAW **(CC2)**
3. FINANCIAL REPORTING AND ANALYSIS **(CC3)**
4. ENTERPRISE RISK MANAGEMENT **(CC4)**
5. COMPUTER SECURITY **(CC5)**

LEVEL II

6. AML/CFT OPERATIONS **(CC6)**
7. AUDIT AND TAX COMPLIANCE (**CC7)**
8. COMPUTER FORENSICS **(CC8)**
9. CYBER LAW AND ETHICS **(CC 9)**
10. DATA SECURITY MANAGEMENT **(CC10)**

LEVEL III

11. CYBER AND ARTIFICIAL INTELLIGIENCE **(CC11)**
12. FINANCIAL CRIME INVESTIGATION **(CC12)**
13. IT PROGRAMMING AND AUDIT **(CC13)**
14 .GOVERNANCE AND ETHICS **(CC14)**

CCCA CURRICULUM IN DETAILS

LEVEL I

1. CYBER SECURITY OPERATIONS

CONTENT

1. INTRODUCTION TO CYBER SPACE

2. CYBER SECURITY TECHNIQUES

3. INVESTIGATING CYBERCRIMES: INTRODUCTION TO CYBER FORENSIC

4. SOME RECENT CYBER SECURITYATTACKS

5. GUIDELINES FOR SECURE PASSWORD, TWO STEP VERIFICATION AND USING FREE ANTIVIRUS

6. CHOOSING BEST BROWSER TO SUIT YOUR REQUIREMENTS

7. GUIDELINES FOR SAFE INTERNET BROWSING

8. WIRELESS SECURITY

9. EMAIL AND SOCIAL MEDIA SECURITY

10. SMART PHONE SECURITY

2. ENTERPRISE LAW

CONTENT

1. INTRODUCTION TO CORPORATE LAW

2. FORMATION AND PROMOTION

3. CORPORATE PERSONALITY AND THE REGISTERED COMPANY

4. THE CONSTITUTION OF THE REGISTERED COMPANY

5. CORPORATE DECISION MAKING

6. CORPORATE TRANSACTIONS

7. CAPITAL

8. SHARES

9. INSIDER DEALING

10. DIRECTORS

11. ACCOUNTS AND AUDITORS

12. COMPANY CHARGES

13. SHAREHOLDER REMEDIES

14. WINDING UP

3. FINANCIAL REPORTING AND ANALYSIS

CONTENT

1. INTRODUCTION TO FINANCIAL REPORTING
2. INTRODUCTION TO FINANCIAL STATEMENTS AND OTHER FINANCIAL REPORTING TOPICS
3. BALANCE SHEET
4. INCOME STATEMENT
5. BASICS OF ANALYSIS
6. LIQUIDITY OF SHORT-TERM ASSETS; RELATED DEBT-PAYING ABILITY
7. LONG-TERM DEBT-PAYING ABILITY
8. PROFITABILITY
9. FOR THE INVESTOR
10. STATEMENT OF CASH FLOWS

4. ENTERPRISE RISK MANAGEMENT

CONTENT

1. ENTERPRISE RISK MANAGEMENT: AN INTRODUCTION AND OVERVIEW
2. A BRIEF HISTORY OF RISK MANAGEMENT
3 ERM AND ITS ROLE IN STRATEGIC PLANNING AND STRATEGY
4 THE ROLE OF THE BOARD OF DIRECTORS AND SENIOR MANAGEMENT IN ENTERPRISE RISK MANAGEMENT
5 BECOMING THE LAMP BEARER: THE EMERGING ROLES OF THE CHIEF RISK OFFICER
6 CREATING A RISK-AWARE CULTURE
7 ERM FRAMEWORKS
8 IDENTIFYING AND COMMUNICATING KEY RISK INDICATORS
9 HOW TO CREATE AND USE CORPORATE RISK TOLERANCE
10 HOW TO PLAN AND RUN A RISK MANAGEMENT WORKSHOP
11 HOW TO PREPARE A RISK PROFILE
12 HOW TO ALLOCATE RESOURCES BASED ON RISK
13 QUANTITATIVE RISK ASSESSMENTS IN ERM
14 MARKET RISK MANAGEMENT AND COMMON ELEMENTS WITH CREDIT RISK MANAGEMENT
15. CREDIT RISK MANAGEMENT
16. OPERATIONAL RISK MANAGEMENT
17. RISK MANAGEMENT: TECHNIQUES IN SEARCH OF A STRATEGY
18 MANAGING FINANCIAL RISK AND ITS INTERACTION WITH ENTERPRISE RISK MANAGEMENT
19 BANK CAPITAL REGULATIONS AND ENTERPRISE RISK MANAGEMENT
20 LEGAL RISK POST-SOX AND THE SUBPRIME FIASCO: BACK TO THE DRAWING BOARD
21. FINANCIAL REPORTING AND DISCLOSURE RISK MANAGEMENT
22. ENTERPRISE RISK MANAGEMENT: LESSONS FROM THE FIELD

23. RATING AGENCIES' IMPACT ON ENTERPRISE RISK MANAGEMENT

24 ESTABLISHING ERM SYSTEMS IN EMERGING COUNTRIES

5. COMPUTER SECURITY

CONTENT

1. BRIEF HISTORY AND MISSION OF INFORMATION SYSTEM SECURITY
2. HISTORY OF COMPUTER CRIME
3. TOWARD A NEW FRAMEWORK FOR INFORMATION SECURITY
4. HARDWARE ELEMENTS OF SECURITY
5. DATA COMMUNICATIONS AND INFORMATION SECURITY
6. LOCAL AREA NETWORK TOPOLOGIES, PROTOCOLS, AND DESIGN
7. ENCRYPTION
8. USING A COMMON LANGUAGE FOR COMPUTER SECURITY INCIDENT INFORMATION
9. PHYSICAL THREATS TO THE INFORMATION INFRASTRUCTURE
10. SOFTWARE DEVELOPMENT AND QUALITY ASSURANCE
11. APPLICATION CONTROLS
12. SECURITY AUDITS
13. DEVELOPING SECURITY POLICIES

LEVEL II

6. AML/CFT OPERATIONS

CONTENT

1. RISK AND METHODS OF MONEY LAUNDERING AND TERRORIST FINANCING
2. FINANCIAL ACTION TASK FORCE (FATF) RECOMMENDATIONS
3. COMPLIANCE STANDARDS FOR ANTI-MONEY LAUNDERING AND COMBATING THE FINANCING OF TERRORISM
4. ANTI-MONEY LAUNDERING/ COMBATING THE FINANCING OF TERRORISM
5. COMPLIANCE PROGRAM CONDUCTING OR SUPPORTING THE INVESTIGATION PROCESS
6. MODELS OF MONEY LAUNDERING

7. AUDIT AND TAX COMPLIANCE

CONTENT

1: AUDIT AND THE REGULATORY ENVIRONMENT

2: INTERNAL AUDIT

3: AUDIT PLANNING

4: AUDIT STRATEGY, AUDIT DOCUMENTATION AND THE WORK OF OTHERS

5: INTERNAL CONTROLS

6: INTRODUCTION TO AUDIT EVIDENCE

7: AUDIT EVIDENCE – PART 2

8: AUDIT PROCEDURES

9: REVIEW PROCEDURES

10 .CORE BUSINESS IN TAXATION

11. GENERAL DESIGN CONSIDERATIONS IN TAXATION

12. PRIMARY PROCESSES IN TAXATION
13. PLANNING AND CONTROL IN TAXATION

8. COMPUTER FORENSICS

CONTENT

1. COMPUTER FORENSICS AND INVESTIGATIONS AS A PROFESSION

2. UNDERSTANDING COMPUTER INVESTIGATIONS.

3. THE INVESTIGATOR'S OFFICE AND LABORATORY.

4. DATA ACQUISITION

5. PROCESSING CRIME AND INCIDENT SCENES

6. CURRENT COMPUTER FORENSICS TOOLS

7. MACINTOSH AND LINUX BOOT PROCESSES AND FILE SYSTEMS.

8. COMPUTER FORENSICS ANALYSIS AND VALIDATION

9. E-MAIL INVESTIGATIONS

10. REPORT WRITING FOR HIGH-TECH INVESTIGATIONS

11. EXPERT TESTIMONY IN HIGH-TECH INVESTIGATIONS

12. ETHICS FOR THE EXPERT WITNESS

9. CYBER LAW AND ETHICS

SECTION ONE: CYBER LAW

1. DEFINITIONS
2. THE RIGHT TO ACCESS LAWS
3. ANONYMITY LAWS
4. DATA PROTECTION LAWS
5. SOFTWARE, INCLUDING ENCRYPTION LAWS
6. MALICIOUS CODE LAWS
7. SPAM LAWS
8. CYBER-HOOLIGANISM LAWS
9. CYBER-STALKING LAWS
10. IDENTITY THEFT LAWS
11. CYBER-TERRORISM LAWS
12. CYBER-WAR LAWS
13. DISTANCE CONTRACTING LAWS
14. INTELLECTUAL PROPERTY LAWS
15. OBSCENE PUBLICATIONS LAWS
16. DIGITAL SIGNATURES LAWS
17. CIVIL LIBERTIES LAWS
18. CIVIL LIABILITY LAWS
19. CIVIL REMEDIES LAWS
20. CRIMINAL LIABILITY LAWS
21. CRIMINAL PENALTIES LAWS
22. SOVEREIGNTY AND JURISDICTION LAWS
23. STANDARDS OF EVIDENCE LAWS
24. TRANS-NATIONAL EXTRADITION LAWS
25. TELECOMMUNICATIONS REGULATION LAWS
26. REGULATORY AND INVESTIGATORY POWERS LAWS
27. DISPUTE RESOLUTION LAWS
28. TREATY SECRETARIAT LAWS

SECTION TWO: CYBER ETHICS

29. ETHICS IN THE CYBER SPACE: AN OVERVIEW
30. CYBER LAW AND CYBER ETHICS: HOW THE TWINS NEED EACH OTHER
31. ETHICS IN THE INFORMATION SOCIETY
32. ARTIFICIAL INTELLIGENCE ETHICS
33. BLOCKCHAIN ETHICS
34. HOMO DEUS: DATAISM AS RELIGION OF DATA
35. BLOCKCHAIN LEGAL REGULATIONS
36. INTERNATIONAL CONVENTION FOR CYBER SPACE AND ETHICAL FRAMEWORKS

10. DATA SECURITY MANAGEMENT

SECTION ONE

1. CONTEXT AND BACKGROUND OF EUROPEAN DATA PROTECTION LAW

2. DATA PROTECTION TERMINOLOGY

3. THE KEY PRINCIPLES OF EUROPEAN DATA PROTECTION LAW

4. THE RULES OF EUROPEAN DATA PROTECTION LAW

5. THE DATA SUBJECT'S RIGHTS AND THEIR ENFORCEMENT

6. TRANSBORDER DATA FLOWS

7. DATA PROTECTION IN THE CONTEXT OF POLICE AND CRIMINAL JUSTICE

8. OTHER SPECIFIC EUROPEAN DATA PROTECTION LAWS

SECTION TWO

9. OPERATING SYSTEM SECURITY
10. INTRUSION DETECTION AND INTRUSION PREVENTION DEVICES
11. IDENTIFICATION AND AUTHENTICATION
12. WEB MONITORING AND CONTENT FILTERING
13. SECURING STORED DATA
14. ANTIVIRUS TECHNOLOGY
15. PROTECTING DIGITAL RIGHTS: TECHNICAL APPROACHES

LEVEL III

11. CYBER AND ARTIFICIAL INTELLIGIENCE

CONTENT

SECTION A: CYBER INTELLIGIENCE

1. DEFINING CYBER THREAT INTELLIGENCE

2. DEVELOPING CYBER THREAT INTELLIGENCE REQUIREMENTS

3. COLLECTING CYBER THREAT INFORMATION

4. ANALYZING AND DISSEMINATING CYBER THREAT INTELLIGENCE

5. USING CYBER THREAT INTELLIGENCE

6. IMPLEMENTING AN INTELLIGENCE PROGRAM

7. SELECTING THE RIGHT CYBER THREAT INTELLIGENCE PARTNER

SECTION B: ARTIFICIAL INTELLIGIENCE

8. INTRODUCTION TO ARTIFICIAL INTELLIGENCE (AI)

9. AI: PROBLEM-SOLVING

10. AI: KNOWLEDGE AND REASONING
11. ROBOTICS

12. PHILOSOPHICAL FOUNDATIONS

13. AI: PRESENT AND FUTURE

12. FINANCIAL CRIME INVESTIGATION

CONTENT

1. FRAUD: AN INTRODUCTION

2. THE ROLES OF THE AUDITOR AND THE FORENSIC ACCOUNTING INVESTIGATOR

3. PSYCHOLOGY OF THE FRAUDSTER
4. FINANCIAL REPORTING FRAUD AND THE CAPITAL MARKETS
5. AUDITOR RESPONSIBILITIES AND THE LAW
6. INDEPENDENCE, OBJECTIVITY, SKEPTICISM
7. FORENSIC INVESTIGATIONS AND FINANCIAL AUDITS: COMPARE AND CONTRAST
8. POTENTIAL RED FLAGS AND FRAUD DETECTION TECHNIQUES
9. INTERNAL AUDIT: THE SECOND LINE OF DEFENSE
10. FINANCIAL STATEMENT FRAUD: REVENUE AND RECEIVABLES
11. FINANCIAL STATEMENT FRAUD: OTHER SCHEMES AND MISAPPROPRIATIONS
12. WHEN AND WHY TO CALL IN FORENSIC ACCOUNTING INVESTIGATORS
13. TEAMING WITH FORENSIC ACCOUNTING INVESTIGATORS
14. POTENTIAL MISSTEPS: CONSIDERATIONS WHEN FRAUD IS SUSPECTED
15. INVESTIGATIVE TECHNIQUES
16. BACKGROUND INVESTIGATIONS
17. THE ART OF THE INTERVIEW
18. ANALYZING FINANCIAL STATEMENTS
19. DATA MINING: COMPUTER-AIDED FORENSIC ACCOUNTING INVESTIGATION TECHNIQUES
20. BUILDING A CASE: GATHERING AND DOCUMENTING EVIDENCE
21. SUPPORTING A CRIMINAL PROSECUTION
22. REPORT OF INVESTIGATION
23. WORKING WITH ATTORNEYS
24. CONDUCTING GLOBAL INVESTIGATIONS
25. MONEY LAUNDERING
26. OTHER DIMENSIONS OF FORENSIC ACCOUNTING
27. LOOKING FORWARD: THE FUTURE OF FORENSIC ACCOUNTING INVESTIGATION

13. IT PROGAMMING AND AUDIT

CONTENT

SECTION A: IT PROGAMMING

1. PROGRAMMING AND PROGRAMMING LANGUAGES
2. TYPES, OPERATORS, AND EXPRESSIONS
3. BRANCHING AND ITERATION
4. FUNCTIONS
5. SCOPE AND EXTENT
6. SOFTWARE DESIGN
7. POINTERS
8. ARRAYS AND STRINGS
9. DYNAMIC MEMORY
10. THE C PREPROCESSOR
11. STRUCTURES AND UNIONS
12. BITWISE OPERATIONS
13. INPUT AND OUTPUT
14. GENERIC PROGRAMMING
15. DATA STRUCTURES
16. C IN THE REAL WORLD

SECTION B: IT AUDIT

17. BASICS OF COMPUTING SYSTEMS
18. IDENTIFYING COMPUTER SYSTEMS
19. INFORMATION SYSTEMS AUDIT PROGRAM
20. INFORMATION SYSTEMS SECURITY POLICIES, STANDARDS, AND/OR GUIDELINES
21. AUDITING SERVICE ORGANIZATION APPLICATIONS
22 .ASSESSING THE FINANCIAL STABILITY OF VENDOR ORGANIZATIONS
23. PHYSICAL SECURITY
24. LOGICAL SECURITY
25. INFORMATION SYSTEMS OPERATIONS
26. CONTROL SELF-ASSESSMENT AND AN APPLICATION IN AN INFORMATION SYSTEMS ENVIRONMENT
27. ENCRYPTION AND CRYPTOGRAPHY
28. CONTEMPORARY INFORMATION SYSTEMS AUDITING CHALLENGES
29. INFORMATION SYSTEMS PROJECT MANAGEMENT AUDITS

14 .GOVERNANCE AND ETHICS

CONTENT

1. ETHICS AND GOVERNANCE

2. ETHICAL PRINCIPLES IN BUSINESS

3. CONCEPTUAL FRAMEWORK OF CORPORATE GOVERNANCE

4. BOARD EFFECTIVENESS - ISSUES AND CHALLENGES

5. BOARD COMMITTEES

6. CORPORATE GOVERNANCE AND SHAREHOLDER RIGHTS

7. CORPORATE GOVERNANCE AND OTHER STAKEHOLDERS

8. RISK MANAGEMENT AND INTERNAL CONTROL

9. CORPORATE GOVERNANCE IN BANKS, INSURANCE AND PUBLIC SECTOR COMPANIES

10. LEGISLATIVE FRAMEWORK OF CORPORATE GOVERNANCE - AN INTERNATIONAL PERSPECTIVE

11. CORPORATE SOCIAL RESPONSIBILITY

12. SUSTAINABILITY

13. CORPORATE SUSTAINABILITY REPORTING FRAMEWORKS

14. LEGAL FRAMEWORK, CONVENTIONS, TREATIES ON ENVIRONMENTAL AND SOCIAL ASPECTS