CERTIFIED DATA PROTECTION OFFICER

INCLUDES

ISO27701 LEAD AUITOR

A BCAA Certification

Brit Certifications and Assessments, UK

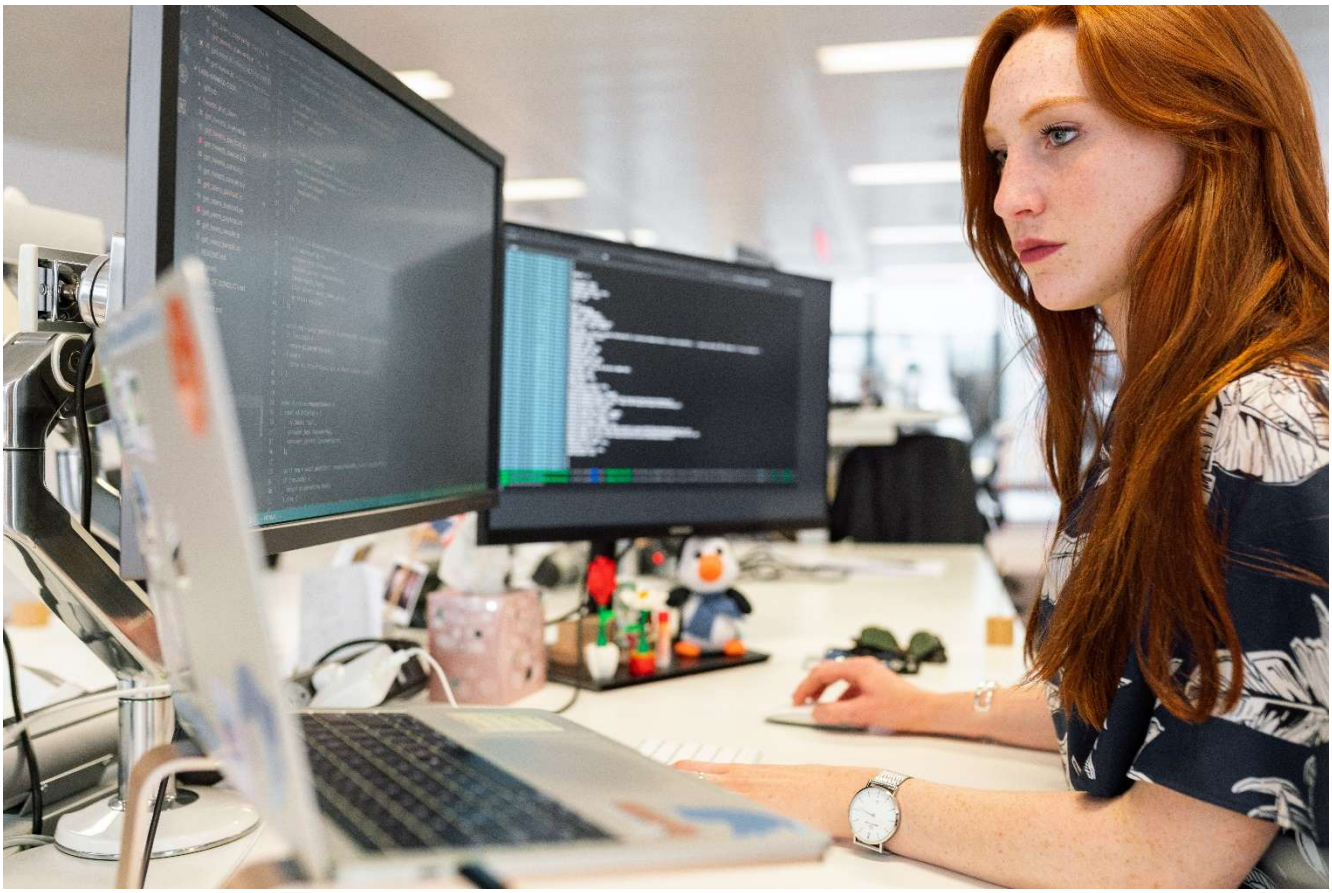
128 City Road, London
EC1V 2NX, United Kingdom

Ph: +44 203 476 4509
enquiry@bcaa.uk

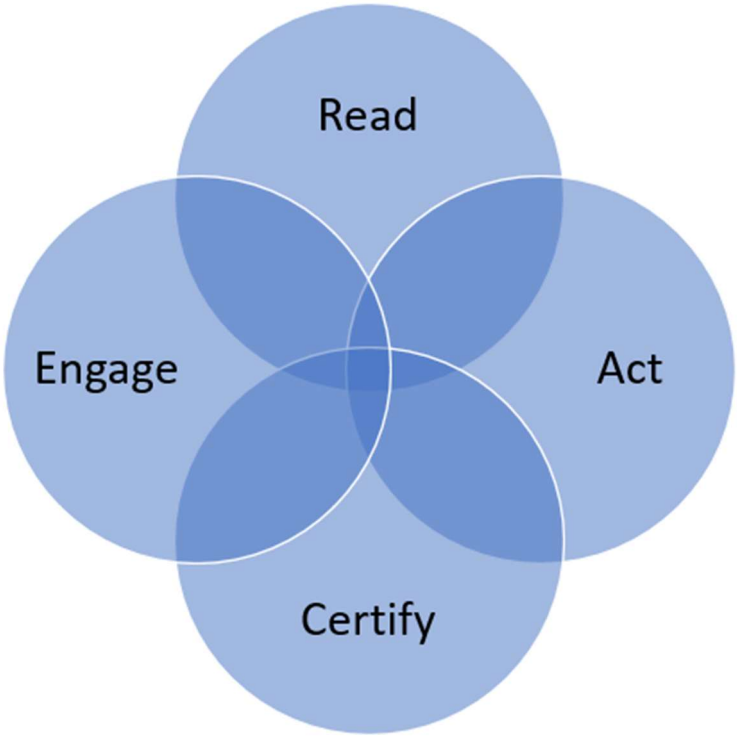
Brit Certifications and Assessments

Brit Certifications and Assessments (BCAA) is a leading UK based certification body. This CB is formed to address the gap in the industry in IT and IT Security sector. The certification body leads in IT security, and IT certifications, and in particular doing it with highly pragmatic way.

BCAA UK works in hub and spoke model across the world.



R A C E Framework



The Read - Act - Certify - Engage framework from Brit Certifications and Assessments is a comprehensive approach designed to guarantee optimal studying, preparation, examination, and post-exam activities. By adhering to this structured process, individuals can be assured of mastering the subject matter effectively. Commencing with the "Read" phase, learners are encouraged to extensively peruse course materials and gain a thorough understanding of the content at hand. This initial step sets the foundation for success by equipping candidates with essential knowledge and insights related to their chosen field. Moving on to the "Act" stage, students actively apply their newfound expertise through practical exercises and real-world scenarios. This hands-on experience allows them to develop crucial problem-solving skills while reinforcing theoretical concepts.

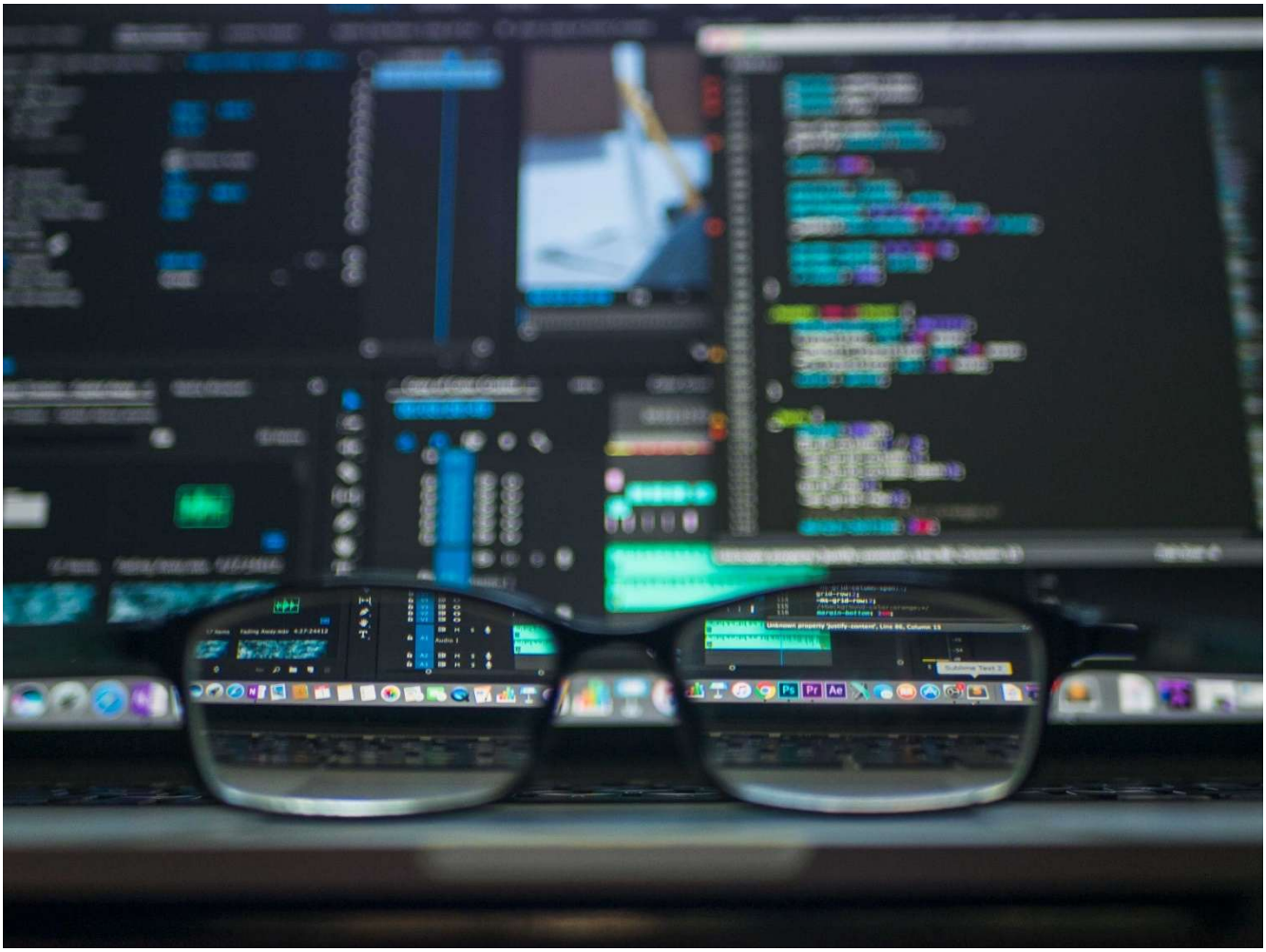
“Certify” stage is where you will take your examination and get certified to establish yourself in the industry. Now “Engage” is the stage in which BCAA partner, will engage you in Webinars, Mock audits, and Group Discussions. This will enable you to keep abreast of your knowledge and build your competence.

Data Protection

Data protection generally means the ability of a person to determine for themselves when, how, and to what extent personal information about them is shared with or communicated to others. This personal information can be one's name, location, contact information, or online or real-world behavior. Just as someone may wish to exclude people from a private conversation, many online users want to control or prevent certain types of personal data collection.

As Internet usage has increased over the years, so has the importance of data privacy. Websites, applications, and social media platforms often need to collect and store personal data about users in order to provide services. However, some applications and platforms may exceed users' expectations for data collection and usage, leaving users with less privacy than they realized. Other apps and platforms may not place adequate safeguards around the data they collect, which can result in a data breach that compromises user privacy.

Certified Chief Data Protection Officer
C-CDPO



Agenda

Module 1: Privacy Compliance Frameworks

- Material scope
- Territorial scope
- Governance
- Objectives
- Key processes
- Personal information management systems
- ISO/IEC 27001:2013
- Selecting and implementing a compliance framework
- Implementing the framework

Module 2: Role of the Data Protection Officer

- Voluntary designation of a Data Protection Officer
- Undertakings that share a DPO
- DPO on a service contract
- Publication of DPO contact details
- Position of the DPO
- Necessary resources
- Acting in an independent manner
- Protected role of the DPO
- Conflicts of interest
- Specification of the DPO
- Duties of the DPO
- The DPO and the organization
- The DPO and the supervisory authority
- Data protection impact assessments and risk management
- In house or contract

Module 3: Common Data Security Failures

- Personal data breaches
- Anatomy of a data breach
- Sites of attack
- Securing your information
- ISO 27001
- Ten Steps to Cyber Security
- Cyber Essentials
- NIST standards
- The information security policy
- Assuring information security
- Governance of information security
- Information security beyond the organisation's borders

Module 4: Six Data Protection Principles

- Principle 1: Lawfulness, fairness and transparency
- Principle 2: Purpose limitation
- Principle 3: Data minimisation
- Principle 4: Accuracy

- Principle 5: Storage limitation
- Principle 6: Integrity and confidentiality
- Accountability and compliance

Module 5: Requirements for Data Protection Impact Assessments

- Data protection impact assessments
- When to conduct a DPIA
- Who needs to be involved
- Data protection by design and by default

Module 6: Risk Management and DPIAs

- DPIAs as part of risk management
- Risk management standards and methodologies
- Risk responses
- Risk relationships
- Risk management and personal data

Module 7: Data Mapping

- Objectives and outcomes
- Four elements of data flow
- Data mapping, DPIAs and risk management

Module 8: Conducting DPIAs

- Reasons for conducting a DPIA
- Objectives and outcomes
- Consultation
- Five key stages of the DPIA
- Integrating the DPIA into the project plan

Module 9: Data Subjects' Rights

- Fair processing
- The right to access
- The right to rectification
- The right to be forgotten
- The right to restriction of processing

- The right to data portability
- The right to object
- The right to appropriate decision making

Module 10: Consent

- Consent in a nutshell
- Withdrawing consent
- Alternatives to consent
- Practicalities of consent
- Children
- Special categories of personal data
- Data relating to criminal convictions and offences

Module 11: Subject Access Requests

- The information to provide
- Data portability
- Responsibilities of the data controller
- Processes and procedures
- Options for confirming the requester's identity
- Records to examine
- Time and money
- Dealing with bulk subject access requests
- Right to refusal

Module 12: Controllers and Processors

- Data controllers
- Joint controllers
- Data processors
- Controllers that are processors
- Controllers and processors outside the EU
- Records of processing
- Demonstrating compliance

Module 13: Managing Personal Data Internationally

- Key requirements

- Adequacy decisions
- Safeguards
- Binding corporate rules
- The EU-US Privacy Shield
- Privacy Shield Principles
- Limited transfers
- Cloud services

Module 14: Incident Response Management and Reporting Notification

- Events vs incidents
- Types of incident
- Cyber security incident response plans
- Key roles in incident management
- Prepare
- Respond
- Follow up

Module 15: GDPR Enforcement

- The hierarchy of authorities
- One-stop-shop mechanism
- Duties of supervisory authorities
- Powers of supervisory authorities
- Duties and powers of the European Data Protection Board
- Data subjects' rights to redress
- Administrative fines
- The Regulation's impact on other laws

Exam

The training is followed by a subjective CDPO open book exam after successful completion of the training.

You need to submit an article on data protection and a video not less than 10 minutes on topics of Data Protection to your partner.

ISO27701 Lead Implementor:

Candidate must participate in ISO27701 mock audit swapping role play as a consultant and auditor to gain ISO27701 Lead Auditor or Implementer certificate.

Topics for Articles:

Article Name
Legal and Regulatory Frameworks
1. The Evolution of GDPR: A Five-Year Retrospective
2. Comparing Data Protection Laws Across Jurisdictions
3. The Impact of CCPA on California Businesses
4. Understanding the EU-US Data Privacy Framework
5. Key Provisions of the Digital Personal Data Protection Bill in India
6. Data Localization Laws: Global Trends and Implications
7. The Role of Data Protection Officers Under GDPR
8. Navigating Cross-Border Data Transfers in a Post-Schrems II World
9. The Right to be Forgotten: Implementation Challenges
10. Consent Management in the Age of Data Protection
Emerging Technologies and Data Protection
11. Blockchain and Data Protection: Opportunities and Challenges
12. AI Ethics and Data Protection: Striking the Right Balance
13. IoT Security: Protecting Personal Data in Smart Devices
14. Biometric Data Protection: Legal and Ethical Considerations
15. Cloud Computing and Data Sovereignty
16. 5G Networks: Data Protection Implications and Safeguards
17. Quantum Computing: Future Threats to Data Encryption
18. Edge Computing and Data Minimization Strategies
19. Data Protection in Virtual and Augmented Reality Environments
20. Protecting Genetic Data: Privacy Concerns in the Genomics Era
Cybersecurity and Data Protection

21. Zero Trust Architecture: A Data Protection Imperative
22. Ransomware Prevention: Best Practices for Data Security
23. Data Breach Notification Laws: A Global Perspective
24. The Role of Encryption in Data Protection Strategies
25. Insider Threats: Mitigating Risks to Sensitive Data
26. Cloud Security: Ensuring Data Protection in Multi-Cloud Environments
27. Mobile Device Management: Balancing Security and Privacy
28. Phishing Prevention: Protecting Personal Data from Social Engineering
29. Secure Coding Practices for Data Protection
30. Vulnerability Management: A Proactive Approach to Data Security
Data Governance and Management
31. Data Minimization: Strategies for Reducing Privacy Risks
32. Data Retention Policies: Balancing Legal Requirements and Privacy
33. Data Classification: A Foundation for Effective Data Protection
34. Privacy by Design: Embedding Data Protection into Business Processes
35. Data Protection Impact Assessments: When and How to Conduct Them
36. Third-Party Risk Management in Data Protection
37. Data Mapping: A Critical Step in GDPR Compliance
38. The Role of Data Protection in Digital Transformation Initiatives
39. Data Quality Management: Ensuring Accuracy and Integrity
40. Data Lifecycle Management: From Creation to Deletion
Industry-Specific Data Protection
41. Healthcare Data Protection: Balancing Privacy and Patient Care
42. Financial Services: Data Protection Challenges in the Digital Age
43. E-commerce and Data Protection: Building Customer Trust
44. Education Sector: Safeguarding Student Data Privacy
45. Telecommunications: Data Protection in the 5G Era
46. Smart Cities: Balancing Innovation and Privacy Protection
47. Data Protection in the Gig Economy: Challenges and Solutions
48. Protecting Personal Data in the Travel and Hospitality Industry
49. Data Protection Considerations for Non-Profit Organizations
50. Media and Entertainment: Balancing Free Speech and Data Privacy
Data Subject Rights and Empowerment
51. Data Portability: Empowering Users in the Digital Economy
52. Automated Decision-Making: Ensuring Fairness and Transparency
53. Children's Data Protection: Special Considerations and Safeguards
54. Data Subject Access Requests: Best Practices for Compliance
55. Privacy Enhancing Technologies: Empowering Individual Data Control
56. Digital Identity Management: Balancing Convenience and Privacy
57. The Right to Explanation: Interpreting AI Decisions
58. Privacy Policies: Effective Communication with Data Subjects
59. Data Protection and Digital Literacy: Educating the Public
60. Privacy-Preserving Data Sharing: Techniques and Applications
Data Protection in Practice
61. Incident Response Planning for Data Breaches
62. Data Protection Training: Fostering a Culture of Privacy
63. Privacy Audits: Assessing and Improving Data Protection Practices
64. Data Protection in Mergers and Acquisitions

65. Anonymization and Pseudonymization Techniques for Data Protection
66. Data Protection in Agile Development Environments
67. Privacy-Preserving Machine Learning: Techniques and Challenges
68. Data Protection Considerations in Customer Relationship Management
69. Implementing Data Loss Prevention (DLP) Solutions
70. Data Protection in Open Source Software Development
International Data Protection
71. APEC Cross-Border Privacy Rules: Facilitating Global Data Flows
72. African Data Protection Landscape: Emerging Trends and Challenges
73. Latin American Data Protection Laws: A Comparative Analysis
74. Data Protection in the Middle East: Evolving Regulatory Frameworks
75. ASEAN Data Protection Framework: Harmonizing Regional Approaches
76. Data Protection in China: Understanding the Personal Information Protection Law
77. Russia's Data Localization Requirements: Implications for Global Businesses
78. Data Protection in Brexit Britain: Divergence from EU Standards?
79. Global Privacy Control: A New Standard for Data Protection?
80. International Data Protection Day: Raising Global Awareness
Future of Data Protection
81. Federated Learning: A Privacy-Preserving Approach to AI
82. Homomorphic Encryption: Processing Encrypted Data Without Decryption
83. Quantum-Resistant Cryptography: Preparing for the Post-Quantum Era
84. Decentralized Identity: Empowering Users in the Digital World
85. Privacy-Preserving Contact Tracing: Lessons from the COVID-19 Pandemic
86. Data Protection in the Metaverse: Anticipating Future Challenges
87. Ethical AI and Data Protection: Shaping the Future of Technology
88. The Role of Data Protection in Combating Disinformation
89. Data Protection and Climate Change: The Environmental Impact of Data Centers
90. The Future of Cookie Consent: Life After Third-Party Cookies
Data Protection and Society
91. Data Protection and Social Justice: Addressing Algorithmic Bias
92. The Economics of Data Protection: Costs and Benefits for Businesses
93. Data Protection in Political Campaigns: Safeguarding Democratic Processes
94. The Role of Data Protection in Combating Cyberbullying
95. Data Protection and Mental Health: Safeguarding Sensitive Information
96. The Intersection of Data Protection and Freedom of Expression
97. Data Protection in Scientific Research: Balancing Progress and Privacy
98. The Impact of Data Protection on Innovation and Competitiveness
99. Data Protection and Digital Divide: Ensuring Equitable Privacy Safeguards
100. The Role of Data Protection in Building Trust in the Digital Economy

Eligibility

- Managers or consultants seeking to prepare and support an organization in planning, implementing, and maintaining a compliance program based on the GDPR
- DPOs and individuals responsible for maintaining conformance with the GDPR requirements
- Members of information security, incident management, and business continuity teams
- Technical and compliance experts seeking to prepare for a data protection officer role
- Expert advisors involved in the security of personal data

Continuous Learning Credits.

The candidates must maintain continuous learning credits, using which the certificate can be renewed with 50 USD at the time of the expiry of the certificate.

The participants are required to maintain 50 CLC credits at the minimum per year.

1. Delivering a webinar (Minimum one hour) – 10 Credits/webinar
2. Participating in a webinar - 3 credits/webinar
3. Participating in a group discussion – 5 credits/GD
4. Giving a interview – 5 credits/Interview
5. Writing an article for BCAA – 10 credits/article
6. Conducting a training for BCAA UK Partner – 3 credits per day

Every candidate needs to maintain a minimum of 60 credits per year for certificate renewal.

Contact

BRIT CERTIFICATIONS AND ASSESSMENTS (UK),
128 City Road, London, EC1V 2NX,
United Kingdom
enquiry@bcaa.uk

‘Together we win.’