

## Benchmarking the (ISC)<sup>2</sup> CISSP qualification



### UK NARIC has found the Certified Information Systems Security Professional (CISSP) certification, awarded by (ISC)<sup>2</sup>, comparable to RQF Level 7<sup>1</sup>

#### Context and scope

(ISC)<sup>2</sup> is a professional membership organisation in the cybersecurity industry based in Florida, in the United States, operating globally with offices in London, Hong Kong and Washington, DC. The CISSP certification is one of a range of certifications offered by (ISC)<sup>2</sup> designed to validate an individual's industry-specific knowledge and skills. In all, (ISC)<sup>2</sup> has over 150,000 certified members worldwide.

In March 2020 UK NARIC completed an independent evaluation and benchmarking of the CISSP in the context of the UK education system to determine its comparable educational level in the UK, and furthering national and international understanding of the CISSP.

#### CISSP qualification

The CISSP is designed for experienced practitioners, managers and executives seeking validation of knowledge and experience in designing, implementing and managing an organisation's cybersecurity.

<sup>1</sup> In terms of how European Qualification Framework (EQF) levels correspond to the RQF, Level 7 on the RQF is referenced to Level 7 in the EQF.

To achieve CISSP certification candidates must pass an examination and have at least five years of cumulative paid work experience<sup>2</sup> in two or more of the eight domains of the (ISC)<sup>2</sup> CISSP Common Body of Knowledge (CBK), which can be completed before the examination or within six years of passing the examination. Candidates taking the latter route are awarded (ISC)<sup>2</sup> Associate status while they complete the work experience component post-examination.

The CISSP examination is a computer-based multiple-choice examination delivered in two forms. The Computer Adaptive Test (CAT)<sup>3</sup> was introduced in December 2017 for candidates taking the CISSP examination in English<sup>4</sup>, and the linear, fixed-form examination is for those taking the exam in French,

<sup>2</sup> Paid / unpaid internships accepted.

<sup>3</sup> CAT's use algorithms during the exam to provide question items based on candidate ability, which reduces the overall number of CISSP questions (approximately 100-150) and maximum length of examination time (three hours) compared to the linear, fixed-form CISSP examination (approximately 250 questions in a maximum time of six hours).

<sup>4</sup> The CISSP CAT exam is not available for delivery in China or South Korea. A list of testing centre locations can be found at: <https://home.pearsonvue.com/Test-takers.aspx>

German, Portuguese, Spanish, Japanese, Simplified Chinese and Korean languages.

The eight domains of the CISSP CBK<sup>5</sup> (Table 1) provide the framework for the assessment of both the CAT and the linear, fixed-form examination, and the five years' required work experience must be in two or more of the domains.

**Table 1: CISSP CBK Domains**

CISSP Domain	Examination weighting (%) <sup>6</sup>
Domain 1: Security and Risk Management	15%
Domain 2: Asset Security	10%
Domain 3: Security Architecture and Engineering	13%
Domain 4: Communication and Network Security	14%
Domain 5: Identity and Access Management (IAM)	13%
Domain 6: Security Assessment and Testing	12%
Domain 7: Security Operations	13%
Domain 8: Software Development Security	10%

Candidates take the CISSP examination at test centres<sup>7</sup> worldwide and can prepare for the exam through various means, including self-study and training courses.<sup>8</sup> Successful completion of the CISSP leads to (ISC)<sup>2</sup> Membership, providing additional membership requirements<sup>9</sup> are met. The CISSP has been found to be recognised by a number of universities (at institutional discretion) across the globe for admissions and/or credit transfer purposes, and there is also evidence of the CISSP CBK domains being integrated into degree programme curricula.

## Methodology

In benchmarking the (ISC)<sup>2</sup> CISSP certification, this study applied UK NARIC's well-established methodology for credential evaluation. This involved a review of core qualification components (i.e. entrance requirements, duration, structure and content, learning outcomes, modes of learning, assessment and

<sup>5</sup> The CISSP CBK refers to the topics relevant to cybersecurity professionals worldwide.

<sup>6</sup> (ISC)<sup>2</sup>, 2018. *CISSP Certified Information Systems Security Professional Certification Exam Outline*. [online, pdf].

<sup>7</sup> Test centres authorised by Pearson VUE, (ISC)<sup>2</sup>'s contracted test provider.

<sup>8</sup> Training is not a requirement to take the examination.

<sup>9</sup> Additional requirements for (ISC)<sup>2</sup> Membership are endorsement of professional experience, being in good standing, agreement to the (ISC)<sup>2</sup> Code of Ethics and payment of (ISC)<sup>2</sup>'s membership fees.

associated outcomes) as well as a comparative analysis of the skills assessed in the CISSP CAT examination to the Regulated Qualifications Framework (RQF) and other suitable reference points<sup>10</sup>, where appropriate. The analysis focused on a sample of retired CAT question items provided by (ISC)<sup>2</sup> for this study. Consideration was also given to (ISC)<sup>2</sup>'s documented quality assurance and control mechanisms for the development and review of the CISSP, including guidelines in place for examination item writers (both CAT and linear-fixed form examination), and for the linear fixed-form examination, the guidelines for translating the items into non-English languages.

## Key findings

The analysis of the CISSP CAT examination question items found knowledge and skills assessment comparable to RQF Level 7 standard, with clear emphasis, for example, on assessing:

- Specialised knowledge, understanding and application skills in the field of cyber security
- Relevant organisational problem-solving and managerial decision-making in different internal and external contexts that are complex and involve many interacting factors, including people and environments that act to mitigate and / or produce change
- Knowledge, understanding and appropriate application and consideration of industrial standards, policy and best practice internationally in the field of cyber security
- Knowledge, understanding and appropriate use of relevant methodologies, techniques and training in cyber security within different business systems and types, including their comparison, analysis, evaluation and measurement.

Certain topic areas and knowledge and skills assessed in the CISSP CAT examination were additionally found to relate well to the content and learning outcomes in similarly-focused Level 7 qualifications. For example, evaluating organisational approaches to information security and advising on appropriate management strategies, while considering the legal, regulatory and societal needs is one such area of commonality. Furthermore, it was found that (ISC)<sup>2</sup> has clear policies and procedures in place regarding development and translation of examination items into the linear fixed-form examination to support the overall comparability of the CISSP to RQF Level 7.

<sup>10</sup> The Framework for Higher Education Qualifications (FHEQ) and similarly-focused qualifications were used as additional reference points, where appropriate.