網絡安全工程技術人才專業能力評價規範

（第一版）

2025-06-30 發佈 2025-06-30 實施

香港網絡空間安全協會 發佈

目 錄

前 言

本文件參考“ISO/IEC 導則，第 2 部分，2018，《ISO 和 IEC 檔的結構和起草的原則與規則》”“ISO/IEC 17024：2012，IDT 合格評定人員認證機構通用要求”“《NICE 網絡安全人才隊伍框架》”“GB/T 42446-2023 網絡安全從業人員能力基本要求”起草，一致性程度為非等效。

本文件由香港網絡空間安全協會提出，香港網絡空間安全協會歸口。

本文件起草單位：香港網絡空間安全協會。

本文件起草人：林小博、成珍苑、程曉峰、龍遠雙。

引　言

為履行《中華人民共和國香港特別行政區維護國家安全法》及《中華人民共和國香港特別行政區個人資料（私隱）條例》所規定的網絡安全責任，亟需建立嚴謹的網絡安全專業人員能力驗證機制。當前，香港特別行政區在網絡安全從業人員能力評價領域缺乏統一標準，制約區域性網絡安全防禦體系的完善與發展。

制定共識性專業能力評價規範，推動權威機構開展網絡安全人才資質評價，可客觀核驗從業人員在以下維度的勝任力：

1.技術知識與應用能力

2.實務經驗與專業業績

3.職業道德與行為準則

從而為人才選拔、職業進階及專業發展提供基準，加速香港網絡安全人才隊伍的專業化及規範化進程。

《網絡安全工程技術人才專業能力評價規範》（Cybersecurity Engineer Professional Competency Assessment Specification，英文縮寫 CECS）在香港特別行政區實施，通過教育訓練、水準考核及多維評價，對證書持有人的綜合素質與技術能力予以權威認定。該規範旨在：

1.確立能力尺規：明確網絡安全從業者的知識、能力與行為準則；

2.驅動人才升級：構建可持續的專業人才發展生態；

3.強化防禦體系：助力國家網絡安全戰略在香港特別行政區的落地實施。

本文件規定網絡安全專業人員的評價體系架構（含類別、級別），並界定評價要求及評價方法，為行業提供可操作的實施框架。

本文件參考 NICE 框架（美）等國際標準，確保人才評價與國際接軌。

1 範圍

本規範為香港網絡空間安全協會（HKCSA）認證人員認證規範類檔。

本規範規定了香港網絡空間安全協會網絡安全工程技術人才專業能力認證遵循的原則。

本規範適用範圍見《網絡安全工程技術人才專業能力認證領域表》，未列入此範圍的其他認證領域按相應的認證檔實施。

網絡安全工程技術人才專業能力認證領域表

序號	認證領域	特定要求
1	網絡與系統安全	附錄 A.1
2	資訊內容安全	附錄 A.2
3	數據安全	附錄 A.3
4	業務安全	附錄 A.4

2 規範性引用檔

ISO/IEC 17024：2012 《合格評定 人員認證機構通用要求》

3 術語和定義

3.1 申請人

提交申請參加認證過程的人員。

3.2 報考人

滿足指定條件且被允許參加認證過程的申請人。

3.3 雇主

雇傭報考人的法律實體。

3.4 證明人

證明報考人工業經曆有效性的個人。

3.5 工作經歷

在相關專業的網絡安全工作中，在監督情況下進行的獲得滿足認證規定技能和知識的工作活動。

3.6 網絡安全工程技術人才

從事網絡安全相關工作的所有人員，包括管理人員、運營人員、技術人員。

4 認證級別

網絡安全工程技術人才共設置四個級別，包括助理級、中級、高級、正高級，助理級最低、正高最高。

4.1 助理級

根據本人申請，經 HKCSA 考核評價，確認符合本規範助理級認證要求的申請人，授予網絡安全工程技術人才助理級認證證書。

4.2 中級

根據本人申請，經 HKCSA 考核評價，確認符合本規範中級認證要求的申請人，授予網絡安全工程技術人才中級認證證書。

4.3 高級

根據本人申請，經 HKCSA 考核評審，確認符合本規範高級認證要求的申請人，授予網絡安全工程技術人才高級認證證書。

4.4 正高級

根據本人申請，經 HKCSA 綜合評審，確認符合本規範正高級認證要求的申請人，授予網絡安全工程技術人才正高級認證證書。

5 基本要求

5.1 申請要求

a) 具有獨立的民事行為能力，具備承擔法律責任的能力，近三年內未受過刑事處罰；

b) 申請人應提供真實、完整的認證資訊、資料。

c) 申請人應簽署聲明，表明同意遵守 HKCSA 網絡安全工程技術人才專業能力評價規範的各項要求，特別是行為規範的要求。

d) 申請人提交完整的認證申請資訊、資料後，HKCSA 開始受理申請。

5.2 考試要求

a) 申請助理級、中級認證的申請人應在 1 年內通過 HKCSA 統一組織的“相應認證領域”水準考試，具有同等資質的申請人可以免考試。

b) 申請高級認證的申請人需通過 HKCSA 統一組織的“相應認證領域”技術工作撰寫與答辯，由 HKCSA 專家委員會考核專業能力及專案經驗。技術工作撰寫與答辯見 HKCSA 相應認證領域考試大綱,具有同等資質的申請人可以免答辯。

c) 考試內容和方式見 HKCSA 相應認證領域考試大綱。

5.3 行為規範要求

a) 遵守中華人民共和國憲法、香港特別行政區基本法、澳門特別行政區基本法及相關法律法規。

b) 遵守網絡安全職業道德規範，認真履行崗位職責，具有高度的社會責任感。

5.4 知識和技能要求

5.4.1 助理級

a) 掌握本專業的基礎理論知識和專業技術知識；

b) 瞭解與本專業相關的法律、法規和政策；

c) 具有獨立完成一般性技術工作的能力；

d) 能處理本專業範圍內一般性技術問題。

5.4.2 中級

a) 熟練掌握並能夠靈活運用本專業基礎理論知識和專業技術知識、業務工作基本方法和技能；

b) 熟悉本專業技術標準和規程，掌握與本專業相關的法律、法規和政策；

c) 瞭解本專業新技術、新工藝、新設備、新材料的現狀和發展趨勢；

d) 具有指導助理級技術人員工作的能力。

5.4.3 高級

a) 系統掌握本專業基礎理論知識和專業技術知識；

b) 掌握與本專業相關的法律、法規和政策；

c) 掌握國內外網絡安全領域現狀和發展趨勢，具有跟蹤網絡安全專業科技發展前沿水準的能力；

d) 認真履行工作職責，履職成效良好，有較高的行業認可度；

e) 在指導、培養中青年學術技術骨幹方面發揮重要作用，能夠指導中級技術人員工作和學習。

5.4.4 正高級

a) 具有全面系統的專業理論知識和實踐功底，全面掌握本專業國內外前沿發展動態，精通與本專業相關的法律、法規和政策；

b) 科研水準、學術造詣或科學實踐能力強，在本專業領域具有很高的知名度和影響力，

c) 在突破關鍵核心技術和自主創新方面做出突出貢獻，發揮較強的引領和示範作用；

d) 在指導、培養中青年學術技術骨幹方面作出突出貢獻，能夠有效指導高級技術人員工作和學習。

6 能力認證要求

6.1 助理級

6.1.1 教育和專業工作經歷要求

具備以下條件之一者，可申報助理級:

a) 具備碩士學位或碩士研究生畢業，從事本專業技術工作；

b) 具備大學本科學歷或技工院校預備技師（技師）班畢業，從事本專業技術工作滿 1 年；

c) 具備副學士學位/大學專科學歷，從事本專業技術工作滿 2 年；

d) 具備中等職業學校畢業學歷，從事本專業技術工作滿 5 年。

注：申請人非香港本地學歷需通過香港學術及職業資歷評審局的學歷評估。

6.1.2 業績要求

申請網絡安全工程技術人才助理級認證的申請人無業績要求。

6.1.3 成果要求

申請網絡安全工程技術人才助理級認證的申請人無成果要求。

6.2 中級

6.2.1 教育和專業工作經歷要求

a) 具備博士學位或博士研究生畢業，從事本專業技術工作；

b) 具備碩士學位或碩士研究生以上學歷，從事本專業技術工作滿 1 年；

c) 具備大學本科學歷或技工院校預備技師（技師）班畢業，從事本專業技術工作滿 4 年，或取的初級職稱後從事本專業技術工作滿 2 年；

d) 具備大學專科或技工院校高級工班以上畢業、取得初級職稱後，從事本專業技術工作滿 4 年；

6.2.2 業績要求

作為參與人能夠參與完成本專業專案的規劃和實施工作，或制定本專業的管理標準、戰略規劃、管理制度，在專案管理、科研開發、技術推廣應用等工作中取得一定成效。

各認證領域的特定專業工作業績要求詳見附錄 A。

6.2.3 成果要求

申請網絡安全工程技術人才中級認證的申請人無成果要求。

6.3 高級

6.3.1 教育和專業工作經歷要求

具備以下條件之一者，可申報高級:

a) 具備博士學位或博士研究生畢業，從事本專業技術工作滿 2 年；

b) 具備碩士學位或碩士研究生畢業，從事本專業技術工作滿 5 年；

c) 具備大學本科及以上學歷或技工院校預備技師（技師）班畢業，取得中級職稱後，從事本專業技術工作滿 3 年；

d) 已取得非本系列（專業）副高級職稱後，從事本專業技術工作滿 3 年。

6.3.2 業績要求

作為主要完成人能夠完成本專業專案的規劃和實施工作，或制定本專業的管理標準、戰略規劃、管理制度，在專案管理、科研開發、技術推廣應用等工作中取得較好成效。

各認證領域的特定專業工作業績要求詳見附錄 A。

6.3.3 成果要求

申請網絡安全工程技術人才高級認證的申請人，應具備下列任何條件 2 項或以上：

a) 作為排名前三的負責人完成業內攻關專案，其研究成果通過行業主管部門鑒定或驗收；

b) 作為排名前三的負責人完成開發新產品、新設備、新工藝等 1 項及以上，並在相關領域實際應用；

c) 作為排名前三完成人獲得已授權的下列之一：發明專利、實用新型專利、電腦軟體著作；

d) 作為主要完成人完成行業內研究報告、評估報告、工程諮詢報告和工程設計檔等，並得到相關部門驗收；

e) 作為排名前三完成人編寫行業內專著或編著，並出版發行；

f) 作為主要完成人發現風險隱患，或作為主持/牽頭處置了安全事件；

g) 作為主要完成人完成技術成果轉移轉化專案，並取得了經濟和社會效益；

h) 作為排名前三的作者在國內外期刊上發表有學術價值的專業論文；

i) 作為排名前三完成人編寫下列之一：國家標準、行業標準、團體標準、地方標準。

6.4 正高級

6.4.1 教育和專業工作經歷要求

具備以下條件者，可申報正高級:

a) 具備大學本科以上學歷，取得高級專業技術認證後，從事本專業技術工作滿 5 年；

各認證領域的特定專業工作經歷要求詳見附錄 A。

6.4.2 業績要求

主持或承擔本專業研究專案、課題，形成的技術報告經同行專家評議具有國內領先水準，並取得顯著經濟或社會效益；或主持制定國家、港特別行政區、行業本專業中長期發展規劃、重大戰略決策等相關政策、標準、規範，並頒佈實施；或作為主持/牽頭發表本專業研究成果，經同行專家評議具有較高學術價值，推動本專業發展。

各認證領域的特定專業工作業績要求詳見附錄 A。

6.4.3 成果要求

申請網絡安全工程技術人才正高級認證的申請人，應具備下列任何條件 3 項或以上：

a) 作為主持/牽頭完成行業內攻關專案，其研究成果通過行業主管部門鑒定或驗收；

b) 作為主持/牽頭完成開發新產品、新設備、新工藝等 1 項及以上，並在相關領域實際應用，取得了經濟和社會效益；

c) 作為第一人獲得已授權的下列之一：發明專利、實用新型專利、電腦軟體著作；

d) 作為主持/牽頭完成行業內較大影響的相關專業研究報告、評估報告、工程諮詢報告和工程設計檔等，並得到相關部門驗收；

e) 作為第一完成人編寫行業內專著或編著，並出版發行；

f) 作為主持/牽頭發現了較大網絡安全風險隱患，或作為主持/牽頭處置了較嚴重網絡安全事件；

g) 作為主持/牽頭完成網絡安全技術成果轉移轉化專案，並取得了經濟和社會效益；

h) 作為第一作者在國內外期刊上發表有學術價值的相關專業論文。

7 證書保持要求

維持認證證書持續有效，證書持有人應滿足以下要求：

a) 遵守網絡安全工程技術人才行為規範；

b) 每年應完成相應專業的繼續教育培訓 16 個學時以上，或參加 HKCSA 認可的行業會議。

8 認證決定與申訴、投訴處理

8.1 認證決定

HKCSA 評價人員根據評價考核過程中收集的資訊形成評價考核結論，給出申請人是否適宜認證的意見。

HKCSA 認證管理人員對評價考核結論、認證意見進行審定，做出是否予以認定的決定。認定管理人員應未參與過對申請人的評價考核與培訓。

HKCSA 秘書長審核認證意見和認證決定，批准認證決定。

8.2 認證公告及認證證書

a) 對已被批准認證/再認證的申請人，HKCSA 將予以公告並頒發/換發認證證書，證書有效期 3 年。對不予認證的申請人，HKCSA 將通知本人。

b) HKCSA 秘書長負責批准認證公告和簽發認證證書。

c) 認證公告包含下列資訊：

----認證人員姓名；

----認證領域；

----認證級別和認證證書編號；

----生效日期。

d) 認證證書包含下列資訊：

----HKCSA 的名稱、標識；

----認證規範資訊；

----認證人員姓名和身份識別資訊；

----認證領域；

----認證級別和認證證書編號。

e) 申請人在取得認證證書之前應簽署《個人聲明》。認證人員在使用認證證書時，應做到：

----僅在獲得認證的領域範圍內使用認證證書，並接受 HKCSA 監督；

----真實、準確的宣傳其認證領域和認證級別；

----不得將認證證書轉交他人使用；

----不得使用失效的認證證書。

f) HKCSA 擁有頒發的各類認證證書的所有權。認證人員證書被暫停期間或撤銷後，不得使用相應證書。

8.3 認定時限

對於符合要求的認定申請,HKCSA 將在 45 個工作日內完成認證批准。因申報資訊和資料不真實、不完整或不符合要求，造成認證過程延遲的時間，不計入認證時限。

8.4 認定收費

HKCSA 依據《網絡安全工程技術人才認證、培訓收費規則》收取認定費用，申請人和已認定人員應遵照規則繳納相應費用。評價和認定過程一經開始，不論認定結果如何，認定費用將不予退還。

8.5 申訴

a) HKCSA 依據《網絡安全工程技術人才認定申訴、投訴與爭議處理程式規則》，處理認定人員的申訴，包括：

----申請人或認定人員對 HKCSA 做出的不予認定、證書處置等決定提出的申訴；

----申訴人因不同意 HKCSA 的投訴處理決定提出的申訴。

b) 申訴應在相關決定做出後 30 天內，以書面形式向 HKCSA 提交。

c) 申訴人可從 HKCSA 網站下載《網絡安全工程技術人才認定申訴、投訴與爭議處理程式規則》，HKCSA 也可應申訴人的請求提供該規則。

8.6 投訴

8.6.1 針對認證人員的投訴

HKCSA 依據《人員認定申訴、投訴與爭議處理程式規則》，處理針對認證人員違反認定要求和行為規範的行為的投訴。

8.6.2 針對 HKCSA 的投訴

a) HKCSA 依據《人員認定申訴、投訴與爭議處理程式規則》，處理針對 HKCSA 工作人員在認定活動中違反工作程式和工作守則的行為的投訴，以及對 HKCSA 的爭議處理決定提出的投訴。

b) 投訴人可從 HKCSA 網站下載《人員認證申訴、投訴與爭議處理程式規則》，HKCSA 也可應投訴人的請求提供該規則。

9 認證證書處置

c) 對違反行為規範、不滿足認證規範要求的各級別技術人員，經調查核實，HKCSA 將按照《認證人員資格處置規則》給予相應處置。

d) 認證人員因個人原因不再保持認證資格的，按照《認證人員資格處置規則》相關條款，可以書面形式向 HKCSA 申請註銷。

附 錄 A

（規範性附錄）

網絡安全工程技術人才特定要求

附錄 A.1 網絡與系統安全專業特定要求

1.專業工作經歷要求

網絡與系統安全專業的專業工作經歷包括從事通信安全、晶片安全、主板安全、記憶體安全、外設安全、嵌入式系統安全、系統軟體安全、雲安全、可信計算與虛擬化安全、網絡與系統安全標準研究與制修訂、網絡與系統安全系統建設、網絡與系統安全系統運維、網絡與系統安全監管、風險評估、惡意代碼分析與防護、事件檢測、漏洞挖掘與逆向分析、系統與網絡安全評測、攻防對抗技術、攻擊行為檢測、分析與處置、應急回應、數據備份、災難恢復、技術成果轉化等工作。

2.專業工作業績要求

2.1 中級

從事網絡與系統安全專業技術工作，熟悉網絡與系統安全的開發流程和建設方法，具備承擔本專業方向的標準制修訂，網絡與系統安全的研發設計、驗證測試、產品開發、軟體開發和應用推廣等相關工作的能力。

2.2 高級

從事網絡與系統安全專業技術工作，系統掌握網絡與系統安全的開發流程和建設方法，具備承擔較複雜的網絡與系統安全的研發設計、驗證測試、產品開發、軟體開發和應用推廣等相關工作的能力。

2.3 正高級

從事網絡與系統安全專業技術工作，全面系統掌握網絡與系統安全的開發流程和建設方法；掌握國內外本專業的技術研發、應用與服務、行業監管和科技成果轉化等的發展動態和發展方向；具備主持完成本專業方向難度很高的研發設計、驗證測試、軟體開發等相關工作的能力；能夠推動本專業的發展，並在領域中所展現出的技術達到國內一流水準。

附錄 A.2 資訊內容安全專業特定要求

1.專業工作經歷要求

資訊內容安全專業的專業工作經歷包括從事多模態資訊獲取與識別、多模態資訊篩選與過濾、資訊內容安全標準研究與制修訂、網絡資訊安全管理、內容理解與輿情分析、資訊與情報分析、資訊挖掘、社交網絡安全、數字版權保護、資訊隱藏、資訊內容審查、資訊內容安全系統評測、資訊內容安全系統建設、資訊內容安全系統運維、資訊內容安全監管、技術成果轉化等工作。

2.專業工作業績要求

2.1 中級

從事資訊內容安全專業技術工作，熟悉資訊內容的獲取、識別、篩選和過濾的技術理論和研究方法；具備承擔本專業方向的資訊內容安全標準制修訂，輿情分析、情報分析、內容評測、資訊挖掘、版權保護、資訊隱藏、內容審查、內容建設、內容運維、技術成果轉讓等相關技術工作的能力。

2.2 高級

從事資訊內容安全專業技術工作，系統掌握資訊內容的獲取、識別、篩選和過濾的技術理論和研究方法，具備承擔較為複雜的輿情分析、情報分析、內容評測、資訊挖掘、版權保護、資訊隱藏、內容審查、內容建設、內容運維、技術成果轉讓等相關技術工作的能力。

2.3 正高級

從事資訊內容安全專業技術工作，全面系統掌握資訊獲取、識別、篩選和過濾的技術理論和研究方法，掌握國內外本專業的技術研發、應用與服務、行業監管和科技成果轉化等的發展動態和發展方向；具備主持完成本專業難度很高的輿情分析、情報分析、內容評測、資訊挖掘、版權保護、資訊隱藏、內容審查、內容建設、內容運維、技術成果轉讓等相關技術工作的能力；能夠推動本專業的發展，並在領域中所展現出的技術達到國內一流水準。

附錄 A.3 數據安全專業特定要求

1.專業工作經歷要求

數據安全專業的專業工作經歷包括從事資料庫安全、身份認證與管理、數據隱私保護、數據分類分級、數據識別與追蹤溯源、安全多方計算、同態加密、隱私計算技術、共識機制安全、智能合約安全、資訊洩漏分析、加密協議軟硬體研發、加密模組安全防護研發、加密產品開發、數據安全與加密標準研究與制修訂、數據安全及加密系統建設、數據安全及加密系統運維、數據安全及加密監管、應用系統規劃、管理、測評與檢查、系統監測、應急演練、事件處置能力評估、技術成果轉化等工作。

2.專業工作業績要求

2.1 中級

從事數據安全專業技術工作，熟悉數據安全識別、跟蹤、評估和治理的技術理論和研究方法，具備承擔本專業方向的標準制修訂，數據安全分析和事後評估、風險治理（數據脫敏、敏感數據歸一化、API 治理、數據資產圖譜、數據加密、隱私管理等）等相關技術工作的能力。

2.2 高級

從事數據安全專業技術工作，系統掌握數據安全識別、跟蹤、評估和治理的技術理論和研究方法，具備承擔較複雜的數據安全分析和事後評估、風險治理（數據脫敏、敏感數據歸一化、API 治理、數據資產地圖、數據加密、隱私管理等）等相關技術工作的能力。

2.3 正高級

從事數據安全專業技術工作，全面系統掌握數據安全識別、跟蹤、評估和治理的技術理論和研究方法；掌握國內外本專業的技術研發、應用與服務、行業監管和科技成果轉化等的發展動態和發展方向；具備主持完成本專業難度很高的數據安全分析和事後評估、風險治理（數據脫敏、敏感數據歸一化、API 治理、數據資產地圖、數據加密、隱私管理等）等相關技術工作的能力；能夠推動本專業的發展，並在領域中所展現出的技術達到國內一流水準。

附錄 A.4 業務安全專業特定要求

1.專業工作經歷要求

業務安全專業的專業工作經歷包括從事電子政務系統安全、電子商務系統安全、電子支付安全、工業控制系統安全、車聯網安全、智慧城市安全、大數據平臺安全、人工智慧安全、軟體定義安全、網絡虛擬化安全、業務安全標準研究與制修訂、業務安全系統建設、業務安全系統運維、業務安全監管、技術成果轉化等工作。

2.專業工作業績要求

2.1 中級

從事業務安全專業技術工作，熟悉新一代電子應用業務的技術理論和研究方法；具備承擔本專業方向的標準制修訂，電子政務、電子商務、電子支付、工業控制、物聯網、智慧城市、人工智慧、軟體定義、網絡虛擬化等業務安全相關技術工作的能力。

2.2 高級

從事業務安全專業技術工作，系統掌握新一代電子應用業務的安全技術理論和研究方法；具備承擔較複雜的電子政務、電子商務、電子支付、工業控制、物聯網、智慧城市、人工智慧、軟體定義、網絡虛擬化等業務安全相關技術工作的能力。

2.3 正高級

從事業務安全專業技術工作，全面系統掌握新一代電子應用業務的安全技術理論和研究方法；掌握國內外本專業的技術研發、應用與服務、行業監管和科技成果轉化等的發展動態和發展方向；具備主持完成本專業難度很高的電子政務、電子商務、電子支付、工業控制、物聯網、智慧城市、人工智慧、軟體定義、網絡虛擬化等業務安全相關技術工作的能力；能夠推動本專業的發展，並在領域中所展現出的技術達到國內一流水準。

附 錄 B

（資料性附錄）

網絡安全工作類別和專業認證對應關係

序號	工作類別	承擔的工作任務	專業能力認證領域
1	網絡安全管理	網絡安全需求分析 網絡安全規劃和管理 網絡數據安全保護 個人資訊保護 密碼技術應用 網絡安全諮詢	可選擇以下之一： 網絡與系統安全專業 數據安全專業 業務安全專業 資訊內容安全專業
2	網絡安全建設	網絡安全需求分析 網絡安全架構設計 網絡安全開發供 應鏈安全管理 網絡安全集成實施 網絡數據安全保護 個人資訊保護 密碼技術應用	
3	網絡安全運營	網絡安全運維 網絡安全監測和分析 網絡安全應急管理 網絡數據安全保護 個人資訊保護 密碼技術應用	
4	網絡安全審計和評估	網絡安全審計 網絡安全測試 網絡安全評估 網絡安全認證 電子數據取證	
5	網絡安全科研教育	網絡安全研究 網絡安全培訓和評價	