








Which ISACA Certification Is Right for You?

	Key Domains	Career Stage	Typical Job Titles for Certification Holders		Experience Required	Labs Included	Recommended Pre-Requisition	Compliments with, to Boost Career
 CISA Certified Information Systems Auditor. <small>An ISAC® Certification</small>	› Information Systems Auditing Process › Governance & Management of IT › Information Systems Acquisition, Development & Implementation › Information Systems Operations & Business Resilience › Protection of Information Assets	› Mid-level IT professionals › IT and internal auditors who audit for information security compliance	› IT Auditor › Compliance Analyst/Program Manager	› Risk Analyst/Program Manager › IT Consultant	Five years of professional information systems auditing, control or security work.	No	› IT Audit Fundamentals certificate	› AAIA › CDPSE › Cybersecurity Fundamentals Certificate › Cloud Auditing Certificate
 AAIA ISACA Advanced in AI Audit.	› AI Governance & Risk › AI Operations › AI Auditing Tools & Techniques	› Mid- to high-level IT professionals	› Senior IT Auditor › Risk Manager › Information Manager	› Chief Information Security › Chief Risk Officer	No additional experience required, but must hold a CISA, CPA or CIA and meet the requirements for those certifications	No	Prerequisites required: › CISA, CPA or CIA	› CDPSE
 CISM Certified Information Security Manager. <small>An ISAC® Certification</small>	› Information Security Governance › Information Security Risk Management › Information Security Program › Incident Management	› Mid- to high-level professionals	› IT Architect › Security Analyst › Data Security Manager	› Security and Compliance Director › VP/AVP Information Security › CIO/CISO/CTO	Five+ years of experience in technical IT security, cybersecurity	No	› CISA › CRISC	› CGEIT
 CRISC Certified in Risk and Information Systems Control. <small>An ISAC® Certification</small>	› Corporate IT Governance › IT Risk Assessment › Risk Response & Reporting › Information Technology & Security	› Mid- to high-level IT professionals	› Risk and Security Manager › IS or Business Analyst › IS Manager › Operations Manager	› Information Control Manager › Chief Information Security or Compliance Officer	One to three years of experience in IT risk and/or security and audit	No	› Early career candidates: IT Risk Fundamentals certificate › CISA certification a plus before starting	› CISM › CGEIT
 CGEIT Certified in the Governance of Enterprise IT. <small>An ISAC® Certification</small>	› Governance of Enterprise IT › IT Resources › Benefits Realization › Risk Optimization	› Highly experienced IT professionals › Advisors to upper management and the board	› CIO, CTO, CISO › Senior IT Internal Auditor, Cybersecurity and Compliance › Lead Analyst—IT Governance, Risk and Compliance	› Security Risk and Compliance Specialist › Information Security Compliance Manager › Governance Risk Consultant	Five+ years of experience in CGEIT domains : › IT Governance › IT Resources › Benefits Realization › Risk Optimization	No	› CISA › CRISC › CISM	› COBIT
 CDPSE Certified Data Privacy Solutions Engineer. <small>An ISAC® Certification</small>	› Privacy Governance › Privacy Risk Management & Compliance › Data Life Cycle Management › Privacy Engineering	› Mid-level IT professionals › Experience in implementing privacy controls	› Data Analyst › Privacy Engineer › Privacy Solutions Architect	› Lead Privacy Manager › IT Consultant	Three to five years of experience in 2+ domains: › Privacy Governance › Privacy Architecture › Data Lifecycle	No	› CISA › CRISC › Data Science Fundamentals	› ISACA Privacy Labs
 CCOA Certified Cybersecurity Operations Analyst. <small>An ISAC® Certification</small>	› Technology Essentials › Incident Detection & Response › Cybersecurity Principles & Risks › Securing Assets › Adversarial Tactics, Techniques & Procedures	› Early- to mid-career professionals	› Cybersecurity Analyst › Information Security Analyst › SOC Analyst	› Vulnerability Analyst › Incident Response Analyst › Tier 1 and 2 SOC Support	Cybersecurity professionals with 2–3 years of experience	Yes: 13 Performance-based labs	› Cybersecurity Fundamentals	› CISM

<https://trainocate.com.my/product-category/isaca/>

CPE Credit Hours:

CPE (Continuing Professional Education) is a key part of maintaining your certification status.

CPE credit hours are optional in Year 1 following initial certification.

To maintain a certification, Years 2+ require you to earn and report:

- › A minimum of 20 CPEs each year
- › A minimum of 120 CPEs over a three-year period
- › Compliance with the ISACA Code of Professional Ethics

Full CPE policies are available at isaca.org