CRISC Certification Application

Applicants who Passed CRISC Exam 2015 and Later

Please use Adobe Reader when filling out this application electronically.

APPLICANT INFORMATION

APPLICANT NAME: _____ ISACA ID: _____

EMAIL: _____ PHONE NUMBER: _____

STEP 1. PASS EXAM

CRISC applicants are required to have passed the CRISC exam in the last five years.
If you have not yet passed the CRISC exam, you can register online at www.isaca.org/examreg

EXAM PASS YEAR: _____

STEP 2. SUBMIT CRISC WORK EXPERIENCE

To qualify for CRISC, you must have 3 years of risk management and information system control experience within the past 10 years of the application submission date.

This experience must be earned in a minimum of two CRISC Job Practice Domains, one of which must be either Domain 1 or 2. The CRISC Job Practice Domains can be found at www.isaca.org/criscjobpractice

Section A: Risk and Information Systems Control Experience

Please list related work experience you are claiming below, beginning with your current or most recent position.
Do not leave dates blank. If you are currently employed, please write today's date for the End Date.

		Dates of Employment *(MM/YY)*		Duration of Experience performing CRISC tasks		CRISC Job Practice Domains *(check all that apply)*			
#	Company Name	Start Date	End Date	Years	Months	1	2	3	4
1									
2									
3									
4									

(minimum 3 years required) **SECTION EXPERIENCE TOTAL**: _____

CRISC Certification Application

Applicants who Passed CRISC Exam 2015 and Later

Please use Adobe Reader when filling out this application electronically.

STEP 3. VERIFY CRISC WORK EXPERIENCE

Using the Experience Verification Form on pages V-1 and V-2 of this application, please ask an employer to verify all experience in Step 2. If your experience includes more than one company, you can obtain additional verification forms at: *www.isaca.org/criscapp*

STEP 4. SUBMIT APPLICATION PAYMENT

All applicants must pay a US $50.00 Application Processing Fee before the application can be fully processed. Submit your payment at: *www.isaca.org/criscpay*

STEP 5. REVIEW AND SIGN TERMS & CONDITIONS AGREEMENT

Continuing Professional Education (CPE) Policy
I hereby apply to Information Systems Audit and Control Association, Inc. (ISACA) for the Certified in Risk and Information Systems Control (CRISC) certification in accordance with and subject to the procedures and policies of ISACA. I have read and agree to the conditions set forth in the Application for Certification and the Continuing Professional Education (CPE) Policy in effect at the time of my application, covering the Certification process and CPE policy.

Code of Ethics
I agree: to provide proof of meeting the eligibility requirements; to permit ISACA to ask for clarification or further verification of all information submitted pursuant to the Application, including but not limited to directly contacting any verifying professional to confirm the information submitted; to comply with the requirements to attain and maintain the certification, including eligibility requirements carrying out the tasks of a CRISC, compliance with ISACA's Code of Ethics, standards, and policies and the fulfillment of renewal requirements; to notify the ISACA certification department promptly if I am unable to comply with the certification requirements; to carry out the tasks of a CRISC; to make claims regarding certification only with respect to the scope for which certification has been granted; and not use the CRISC certificate or logos or marks in a misleading manner or contrary to ISACA guidelines.

Truth in Information
I understand and agree that my Certification application will be denied and any credential granted me by ISACA will be revoked and forfeited in the event that any of the statements or answers provided by me in this application are false or in the event that I violate any of the examination rules or certification requirements. I understand that all certificates are owned by ISACA and if my certificate is granted and then revoked, I will destroy the certificate, discontinue its use and retract all claims of my entitlement to the Certification. I authorize ISACA to make any and all inquiries and investigations it deems necessary to verify my credentials and my professional standing.

3rd Party Information Sharing
I acknowledge that if I am granted the Certification, my certification status will become public, and may be disclosed by ISACA to third parties who inquire. If my application is not approved, I understand that I am able to appeal the decision by contacting ISACA. Appeals undertaken by a Certification exam taker, Certification applicant or by a certified individual are undertaken at the discretion and cost of the examinee or applicant. By signing below, I authorize ISACA to disclose my Certification status. This contact information will be used to fulfill my Certification inquiries and requests.

Contact Policy
By signing below, I authorize ISACA to contact me at the address and numbers provided and that the information I provided is my own and is accurate. I authorize ISACA to release confidential Certification application and certification information if required by law or as described in ISACA's Privacy Policy. To learn more about how we use the information you have provided on this form, please read our Privacy Policy, available at www.isaca.org/privacy.

Usage Agreement
I hereby agree to hold ISACA, its officers, directors, examiners, employees, agents and those of its supporting organizations harmless from any complaint, claim, or damage arising out of any action or omission by any of them in connection with this application; the application process; the failure to issue me any certificate; or any demand for forfeiture or re-delivery of such certificate. Notwithstanding the above, I understand and agree that any action arising out of, or pertaining to this application must be brought in the Circuit Court of Cook County, Illinois, USA, and shall be governed by the laws of the State of Illinois, USA.

I understand that the decision as to whether I qualify for certification rests solely and exclusively with ISACA and that the decision of ISACA is final.

I have read and understand these statements and I intend to be legally bound by them.

APPLICANT SIGNATURE: _____ DATE: _____

STEP 6. SUBMIT APPLICATION

Please submit your application and verification form(s) online at: *https://support.isaca.org*
Select **Certifications & Certificate Programs** and **Submit an Application**.

Submitted applications take approximately two-to-three weeks to process. Upon approval, you will be notified via email. A certification packet, including a letter of approval, a CRISC Certificate, and a metal CRISC pin, will be sent to you via postal mail to the primary address in your MyISACA Profile at: *www.isaca.org/myisaca*. Please allow four-to-eight weeks for delivery.

CRISC Experience Verification Form

Applicants who Passed CRISC Exam 2015 and Later

Please use Adobe Reader when filling out this application electronically.

APPLICANT DETAILS

APPLICANT NAME: _____ ISACA ID: _____

FORM INSTRUCTIONS FOR VERIFIER

The applicant (named above) is applying for CRISC certification through ISACA. ISACA requires the applicant's work experience to be independently verified by a supervisor or manager with whom they have worked. Verifiers cannot be immediate or extended family, nor can they work in the Human Resources department.

You must attest to the applicant's work experience as noted on their attached application form (page A-1) and as described by the CRISC Job Practice Domains and task statements (page V-2).

Please return the form to the applicant for their submission. For any questions, please contact ISACA at https://support.isaca.org or +1.847.660.5505.

VERIFIER INFORMATION

VERIFIER NAME: _____

COMPANY NAME: _____ JOB TITLE: _____

EMAIL: _____ WORK NUMBER: _____

VERIFIER QUESTIONS

1. I am attesting to the following work experience earned by the applicant, as indicated on page A-1 (*check all that apply*):

☐ Section A: Company 1
☐ Section A: Company 2
☐ Section A: Company 3
☐ Section A: Company 4

2. I am attesting to experience during the following duration:

START DATE: _____ END DATE: _____

3. I have functioned in the following role(s) to the applicant:

☐ Supervisor ☐ Manager ☐ Colleague ☐ Client

4. I can also attest that the tasks performed by the applicant, as listed on page V-2 of this form, are correct to the best of my knowledge.

☐ Yes ☐ No

VERIFIER AGREEMENT

I hereby confirm that the information on page V-1 and V-2 is correct to the best of my knowledge and there is no reason this applicant should not be certified in risk and information systems control. I am also willing, if required, to answer questions from ISACA about the above information.

VERIFIER SIGNATURE: _____ DATE: _____

CRISC Experience Verification Form
Applicants who Passed CRISC Exam 2015 and Later

Please use Adobe Reader when filling out this application electronically.

JOB PRACTICE DOMAIN INSTRUCTIONS

Applicant is required to check any domain in which any or all tasks have been completed.

☐ DOMAIN 1 - IT Risk Identification

Identify the universe of IT risk to contribute to the execution of the IT risk management strategy in support of business objectives and in alignment with the enterprise risk management (ERM) strategy.

Task Statements:

- Collect and review information, including existing documentation, regarding the organization's internal and external business and IT environments to identify potential or realized impacts of IT risk to the organization's business objectives and operations.
- Identify potential threats and vulnerabilities to the organization's people, processes and technology to enable IT risk analysis.
- Develop a comprehensive set of IT risk scenarios based on available information to determine the potential impact to business objectives and operations.
- Identify key stakeholders for IT risk scenarios to help establish accountability.
- Establish an IT risk register to help ensure that identified IT risk scenarios are accounted for and incorporated into the enterprise-wide risk profile.
- Identify risk appetite and tolerance defined by senior leadership and key stakeholders to ensure alignment with business objectives.
- Collaborate in the development of a risk awareness program, and conduct training to ensure that stakeholders understand risk and to promote a risk-aware culture.

☐ DOMAIN 2 - IT Risk Assessment

Analyze and evaluate IT risk to determine the likelihood and impact on business objectives to enable risk-based decision making.

Task Statements:

- Analyze risk scenarios based on organizational criteria (e.g., organizational structure, policies, standards, technology, architecture, controls) to determine the likelihood and impact of an identified risk.
- Identify the current state of existing controls and evaluate their effectiveness for IT risk mitigation.
- Review the results of risk and control analysis to assess any gaps between current and desired states of the IT risk environment.
- Ensure that risk ownership is assigned at the appropriate level to establish clear lines of accountability.
- Communicate the results of risk assessments to senior management and appropriate stakeholders to enable risk-based decision making.
- Update the risk register with the results of the risk assessment.

☐ DOMAIN 3 - Risk Response and Mitigation

Determine risk response options and evaluate their efficiency and effectiveness to manage risk in alignment with business objectives.

Task Statements:

- Consult with risk owners to select and align recommended risk responses with business objectives and enable informed risk decisions.
- Consult with, or assist, risk owners on the development of risk action plans to ensure that plans include key elements (e.g., response, cost, target date).
- Consult on the design and implementation or adjustment of mitigating controls to ensure that the risk is managed to an acceptable level.
- Ensure that control ownership is assigned to establish clear lines of accountability.
- Assist control owners in developing control procedures and documentation to enable efficient and effective control execution.
- Update the risk register to reflect changes in risk and management's risk response.
- Validate that risk responses have been executed according to the risk action plans.

☐ DOMAIN 4 - Risk and Control Monitoring and Reporting

Continuously monitor and report on IT risk and controls to relevant stakeholders to ensure the continued efficiency and effectiveness of the IT risk management strategy and its alignment to business objectives.

Task Statements:

- Define and establish key risk indicators (KRIs) and thresholds based on available data, to enable monitoring of changes in risk.
- Monitor and analyze key risk indicators (KRIs) to identify changes or trends in the IT risk profile.
- Report on changes or trends related to the IT risk profile to assist management and relevant stakeholders in decision making.
- Facilitate the identification of metrics and key performance indicators (KPIs) to enable the measurement of control performance.
- Monitor and analyze key performance indicators (KPIs) to identify changes or trends related to the control environment and determine the efficiency and effectiveness of controls.
- Review the results of control assessments to determine the effectiveness of the control environment.
- Report on the performance of, changes to, or trends in the overall risk profile and control environment to relevant stakeholders to enable decision making.