CRISC Certification Application
Applicants who Passed CRISC Exam August 2021 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/credentialing/crisc#register.
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 Domains, one of which must be either Domain 1 or 2. The CRISC Domains can be found at: https://www.isaca.org/credentialing/crisc/crisc-exam-content-outline.

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.

<table>
<thead>
<tr>
<th>#</th>
<th>Company Name</th>
<th>Start Date (MM/YY)</th>
<th>End Date (MM/YY)</th>
<th>Years</th>
<th>Months</th>
<th>CRISC Domains (check all that apply)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1 2 3 4</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

(minimum 3 years required) SECTION EXPERIENCE TOTAL: _______
CRISC Certification Application
Applicants who Passed CRISC Exam August 2021 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 pages by downloading the application form at: https://www.isaca.org/credentialing/crisc/get-crisc-certified.

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/bookstore/certification-related-products/crisc_app.

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-policy.

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: ________________

A handwritten signature or verifiable digital signature is required.

STEP 6. SUBMIT APPLICATION
Please submit your application and verification form(s) online at: https://isaca.force.com/support/s/application-submission.

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 August 2021 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 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 3
☐ Section A: Company 2 ☐ 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: ________________

A handwritten signature or verifiable digital signature is required.
CRISC Experience Verification Form
Applicants who Passed CRISC Exam August 2021 and Later

Please use Adobe Reader when filling out this application electronically.

**EXAM CONTENT OUTLINE DOMAIN INSTRUCTIONS**

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

### DOMAIN 1 - Governance (Organizational Governance, Risk Governance)

**Task Statements:**
- Outline how the key concepts of risk impact the enterprise.
- Distinguish between governance and management functions.
- Describe the relationship between enterprise risk and IT risk.
- Define roles and responsibilities within the organizational structure and explain how they relate to risk management.
- Outline the impact of organizational culture on risk management.
- Identify organizational assets and how they are valued.
- Explain how policies and standards provide direction to the enterprise.
- Describe how the business process reviews help improve enterprise effectiveness.
- Describe the concepts of enterprise risk management.
- Assess risk frameworks and their role enterprise risk management.
- Explain role of the risk practitioner in the three lines of defense.
- Define the types of risk profiles.
- Describe the relationship between risk appetite and risk tolerance.
- Describe the impact of legal, regulatory, and contractual obligations regarding risk management.
- Explain the importance of professional ethics in risk management.

### DOMAIN 2 - IT Risk Assessment (IT Risk Identification, IT Risk Analysis and Evaluation)

**Task Statements:**
- Define the types of risk events and threats an enterprise can face.
- Explain the risk identification process.
- Identify threat modeling techniques.
- Compile a threat profile using threat modeling techniques.
- Describe the process and benefits of developing risk scenarios.
- Explain the risk assessment process.
- Define common risk assessment standards and frameworks.
- Describe the value of the risk register to the enterprise.
- Explain risk analysis methodologies and how they are used.
- Illustrate the relationship between business impact analysis and risk assessment.
- Outline the effect of inherent and residual risk on the enterprise.

### DOMAIN 3 - Risk Response and Reporting (Risk Response, Control Design and Implementation, Risk Monitoring and Reporting)

**Task Statements:**
- Determine roles accountable for risk and control ownership.
- Align risk treatment and response options with enterprise risk appetite and tolerance.
- Address risk originating from outside the enterprise (or from third parties).
- Apply procedures to processes and functions containing high amounts of variability.
- Evaluate emerging technologies and changes to the environment for threats, vulnerabilities and opportunities.
- Categorize controls relative to the type of risk response required.
- Leverage common standards and frameworks in designing and implementing controls.
- Identify the current state of existing controls and evaluate their effectiveness for IT risk mitigation.
- Assess gaps between current and desired states of the IT risk environment.
- Collaborate with control owners on the selection, design and implementation of controls.
- Conduct aggregation, analysis and validation of risk and control data.
- Validate risk responses have been executed according to risk treatment plans.
- Describe the types of risk data available to monitor and report risk.
- Identify types of control assessments.
- Explain the process of compiling and reporting the status of controls.
- Apply the steps of control monitoring process.
- Establish a process to define, monitor and analyze metrics relevant to enterprise risk.

### DOMAIN 4 - Information Technology and Security (Information Technology Principles, Information Security Principles)

**Task Statements:**
- Explain the key components of enterprise architecture and the frameworks used to implement them.
- Identify IT components and their areas of concern relating to enterprise risk.
- Describe the project risk and how it is addressed in the project management process.
- Outline the steps and requirements needed to maintain enterprise resiliency.
- Assess areas of risk throughout the data life cycle.
- Articulate key security and support tasks to perform during the system development life cycle.
- Evaluate emerging technologies and changes to the environment for threats, vulnerabilities and opportunities.
- Identify factors that can impact security and risk in the enterprise.
- Leverage information security frameworks and standards to manage information systems and data.
- Review the scope of information security training and awareness programs against identified threats faced by the enterprise.
- Apply data privacy and data protection principles to risk assessment activities.