



**Certified in Risk
and Information
Systems Control™**

An ISACA® Certification

Application for CRISC Certification

**For individuals who passed
a CRISC exam administered in 2015 or later.**



Trust in, and value from, information systems

Requirements to Become a Certified in Risk and Information Systems Control (CRISC)

THIS APPLICATION IS TO BE USED FOR THOSE INDIVIDUALS WHO TOOK AND PASSED A CRISC EXAM ADMINISTERED IN 2015 OR LATER.

To become Certified in Risk and Information Systems Control (CRISC), an applicant must:

1. Score a passing grade on the CRISC exam. A passing score on the CRISC exam, without completing the required work experience as outlined below, will only be valid for five years. If the applicant does not apply or meet the CRISC certification requirements within the five year period, the passing score will be voided.

Important Note: Your completed CRISC application for certification must be submitted within 5 years from the date of initially passing the examination. Retaking and passing the examination will be required if the (completed) application for certification is not submitted within five years from the passing date of the examination.

2. Submit payment for the CRISC application processing fee of US \$50 online at www.isaca.org/criscpay.
3. Submit verified evidence of at least three years of cumulative work experience in IT risk and information systems (IS) control as described in the job practice. In addition, this experience must be earned in at least two domains, one of which must be in either domain 1 or 2.
 - There are no substitutions or experience waivers.
 - Work experience must be gained within the ten year period preceding the application date for certification or within five years from the date of initially passing the exam.
4. Agree to abide by the ISACA Code of Professional Ethics.
5. Agree to abide by the CRISC Continuing Education Policy, which can be viewed at www.isaca.org/crisccpepolicy.

ISACA Code of Professional Ethics

ISACA sets forth a Code of Professional Ethics to guide the professional and personal conduct of ISACA members and credential holders. To view a copy of the code please visit: www.isaca.org/ethics.

CRISC Continuing Professional Education (CPE) Policy

CRISC certified professionals are required to remain current with new practices, trends, and technologies by adhering to the CRISC CPE policy. As such, each individual must maintain an adequate level of current knowledge and proficiency in business and information technology risk and control practices. Those who successfully comply with the continuing professional education policy will be better equipped to support their Board of Directors and executive management. To view a copy of the policy please visit: www.isaca.org/crisccpepolicy.

Instructions for Completing and Submitting Your Application and Documentation

Carefully follow the instructions to complete your application. Be sure to complete all appropriate sections and sign your application.

Incomplete or unsigned applications will not be accepted. Applications will be randomly selected for audit of the verification forms.

In order for your application to be processed, you **MUST** collect your verification of work experience forms and submit with your application via mail, FAX, or e-mail to:

CRISC Certification
ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Fax: +1.847.253.1755
Email: application@isaca.org

Instructions for Completion of the Application

Applicant Information

Complete the top section of pages A-1 and A-2 with your name, ISACA ID number (ID#), email address and phone number.

Section 1—Employment History

For each employer (starting with the most current), enter the following information:

- Employer (Company) Name. Enter the name of the employer (company) where CRISC tasks were performed. Use one assessment box for each employer.
- CRISC Domain Work Experience. **For each domain** in which you earned experience, enter the period of time (in the From MM/YY and To MM/YY boxes) that you performed tasks within the domain (see page V-2 for domains and task statements), and the years/months of experience that you are claiming with this employer. Do not leave dates blank. If currently employed, include a date or current, now, present, etc. To qualify you need 3 years of cumulative experience across a minimum of 2 domains, one of which must be in either domain 1 or 2.

Example: If in 2011 and 2012, you worked the entire year in domains 1 and 2 with this company and in 2013 you only worked in domain 4 for the entire year for an employer, you would enter:

<u>CRISC Domain Experience</u>	<u>From MM/YY</u>	<u>To MM/YY</u>	<u>YEARS</u>	<u>MONTHS</u>
Domain 1	1/11	12/12	2	0
Domain 2	1/11	12/12	2	0
Domain 3	-	-	-	-
Domain 4	1/13	12/13	1	0

Total: 3 years (2011, 2012, 2013) cumulative experience.

Total: Do not add column figures; your total experience is the actual ‘length of time’ working in all the domains. Total years/months of experience cannot exceed the total length of employment with this employer. In the example above your total length of time in all the domains is 3 years (2011-2013) NOT column total of 5 years.

- **The total years/months of experience cannot exceed the total length of employment with this employer.**
- Repeat these steps for each employer for which you are claiming CRISC experience.
- If you are using more than 3 employers, please print out additional copies of page A-1.

Section 2—Employment Summary

- Total CRISC domain related experience. Add the number of total years and months of CRISC domain experience for each employer. This number must total 3 years or more and you must have experience in at least 2 CRISC domains, one of which must be in either domain 1 or 2.

Section 3—Verifier Information

- For each employer listed in section 1 (page A-1), enter the employer (company) name, verifier name, verifier job title, email address, and business phone of the person who will attest to your work experience at that employer. The employer name typically is identical to the employer name listed in section 1. The individual verifying the work experience must be an independent verifier and not of any relation to the applicant nor can the applicant verify his/her own work. This verifier should be your immediate supervisor or a person of higher position within the organization. It is also acceptable for a knowledgeable client or colleague to verify your work experience if you are self-employed or if your supervisor is unable to do so. It is not acceptable for you as the applicant to also be a verifier on your own experience. Human Resource (HR) verifications for work experience are not acceptable unless applicant directly reports to HR function. Letters of Employment are not acceptable as verification for your work experience.
- Read the acknowledgement. Print and sign your name and date the application form at the bottom of page A-2 with a hand written signature and enter date on form at bottom of page. True digital signatures (those authentically validated) are acceptable. Signatures cut and pasted into the document, imported in a word text box or computer keyed/typed in are **NOT** acceptable. Your application is not complete and will not be accepted unless you have signed and dated this page.

Verification of Work Experience Form (Pages V-1 and V-2)

For each verifier, complete the top portion of the Verification of Work Experience Form page V-1 with your name (applicant name), ISACA ID#, email address and phone number. On the Verification of Work Experience Form V-2, complete the top portion with your name (applicant name), ISACA ID#, and verifier name.

Section 4—Request for Work Experience Verification

You are required to have all of the work experience you claimed in section 1 verified by a person(s) qualified to do so. As mentioned in Section 3 above, this person should be your immediate supervisor or a person of higher position within your organization. It is also acceptable for a knowledgeable client or colleague to verify your work experience if you are self-employed or if someone at your employer is unable to do so. It is not acceptable for you to be a verifier of your own experience. Human Resource (HR) verifications for work experience are not acceptable unless applicant directly reports to HR function. Letters of Employment are not acceptable as verification for your work experience. If you have held multiple positions during the time covered by the application, it is up to the verifier to determine if he/she is able to verify your previous experience. If he/she cannot, an additional verifier(s) will be needed to verify previous experience.

- Print your name (applicant printed name) in the request for work experience verification section. Review the request for work experience verification section and sign and date where indicated (at applicant signature and date) with a hand written signature.
- Check the box of the CRISC tasks on page V-2 that you have performed for each employer and for which that verifier is attesting.
- Provide this form (both pages V-1 and V-2) along with a copy of your completed application (page A-1 only) to each person(s) verifying your specific work experience. It is suggested that you sit with each verifier in order to confirm the tasks that you are claiming to have performed on your application.

Section 5—Verification of Work Experience

This section should be completed by each individual who you have chosen to verify your work experience.

- Ask each verifier to complete their verifier name, professional title, company name, address, verifier e-mail and verifier telephone number.
- From Section 1, ask each verifier to identify which company he/she is verifying work experience for from the employment history boxes (1 or 2 or a combination thereof). For example, if the verifier is verifying experience from the employer in Box 1 only, he/she should record Box 1. If the verifier is verifying experience from the employer in Box 1 and 2, he/she should record Box 1 and Box 2.
- Ask each verifier to review the forms that you provided, including your completed application (page A-1 only) and the CRISC job practice task statement boxes that you checked on page V-2.
- Ask each verifier to answer ALL six questions by putting check marks in the appropriate boxes.
- Ask the verifier to sign and date page V-1 of the verification form. If additional copies are required, photocopy the forms.

VERY IMPORTANT: Collect and send all completed verification forms together with your signed application. **DO NOT SEND THEM SEPARATELY.** Submit completed application and support documents via fax, e-mail or mail to:

Certification Coordinator

ISACA

3701 Algonquin Road, Suite 1010

Rolling Meadows, IL 60008-3124 USA

E-mail: application@isaca.org

Telephone: +1.847.660.5660

Fax: +1.847.253.1443

Please note that verification forms are subject to a random audit. If selected verifiers will be contacted to confirm their completion and verification of the work experience that was verified.

Frequently Missed Items

Incomplete applications stall the process. In addition to the review of your application, you may want to review the items below to ensure that you have these areas covered in your application.

- Applicant has signed/dated pages A-2 and V-1 of the application in ink?
- Do not leave dates of employment blank. If currently employed, include a date or current, now, present, etc.
- Employment dates do not overlap in Section 1 on page A-1.
- Verifier has answered all questions on page V-1 and signed/dated at the bottom of page V-1.
- Applicant and verification signatures on forms must be manually handwritten or digital (authentically validated) signatures. Signatures cut and pasted into the documents, imported in a word text box or computer keyed/typed in are not acceptable.
- Check to confirm that the verifier listed all the employer/companies that he/she is verifying in the box provided on page V-1.
- The work experience used in your application must be gained within the ten year period preceding the application date for certification or within 5 years from the date of initially passing the exam.
- USD\$50 application processing fee has been paid online at www.isaca.org/criscpay.

Follow Your Application Progress

Once you submit your application, you can follow the progress online at MyISACA > MyCertifications page of the web site.

If status shows:	Comment:
Application Link and Last Date to Apply for Certification	Application has not been received or logged into the record.
Unreviewed	Application has been received but not yet sent through for review.
Complete Under Review	Application is going through the review process. An email message will be sent if any additional information/documents are needed to complete your application.
Complete Pending Audit	Application was selected for a random verifier audit and ISACA is awaiting response from the verifier.
Incomplete	The application is incomplete or has missing documents. Email message is sent to the applicant with details on the incomplete or missing items.
Approved	Application has been tentatively approved and will be certified in the next grouping or certifying batch for that certification unless selected for the random verification audit.

Applicant Information

Applicant Name _____ ISACA ID# _____
Last/Family Name First/Given Name Middle Initial

Maiden Name or Former Name(s) _____

Email address _____ Phone number _____

Section 1—Employment History

CRISC certification requires 3 years of cumulative experience across a minimum of 2 domains, one of which must be in either domain 1 or 2. Your CRISC work experience must be gained within the ten year period preceding the application date for certification or within 5 years from the date of initially passing the exam. Work experience greater than 10 years cannot be claimed on your application. Do not leave dates blank. If currently employed, include a date or current, now, present, etc.

Box 1. EMPLOYER (COMPANY) NAME					For each CRISC domain in which you earned experience, enter the period of time (in the From MM/YY and To MM/YY boxes) you performed the tasks (see V-2 for domains and task statements), and the years/months of experience that you are claiming with this employer. See instructions for an example. * Total: Do not add column figures; your total experience is the 'length of time' in all the domains. Total years/months of experience cannot exceed the total length of employment with this employer.
CRISC Domain Work Experience	From MM/YY	To MM/YY	YEARS	MONTHS	
Domain 1 (RI)					
Domain 2 (RA)					
Domain 3 (RRM)					
Domain 4 (RCMR)					
TOTAL*					

Box 2. EMPLOYER (COMPANY) NAME					For each CRISC domain in which you earned experience, enter the period of time (in the From MM/YY and To MM/YY boxes) you performed the tasks (see V-2 for domains and task statements), and the years/months of experience that you are claiming with this employer. See instructions for an example. * Total: Do not add column figures; your total experience is the 'length of time' in all the domains. Total years/months of experience cannot exceed the total length of employment with this employer.
CRISC Domain Work Experience	From MM/YY	To MM/YY	YEARS	MONTHS	
Domain 1 (RI)					
Domain 2 (RA)					
Domain 3 (RRM)					
Domain 4 (RCMR)					
TOTAL*					

Box 3. EMPLOYER (COMPANY) NAME					For each CRISC domain in which you earned experience, enter the period of time (in the From MM/YY and To MM/YY boxes) you performed the tasks (see V-2 for domains and task statements), and the years/months of experience that you are claiming with this employer. See instructions for an example. * Total: Do not add column figures; your total experience is the 'length of time' in all the domains. Total years/months of experience cannot exceed the total length of employment with this employer.
CRISC Domain Work Experience	From MM/YY	To MM/YY	YEARS	MONTHS	
Domain 1 (RI)					
Domain 2 (RA)					
Domain 3 (RRM)					
Domain 4 (RCMR)					
TOTAL*					

Section 2—Employment Summary

TOTAL CRISC overall domain related experience: Must be 3 or more years of cumulative experience across 2 CRISC domains, one of which must be in either domain 1 or 2.	YEARS	MONTHS

Verification of Work Experience Form (page 1 of 2)

Applicant Name _____ ISACA ID# _____
Last/Family Name First/Given Name Middle Initial

E-mail address _____ Phone number _____

Section 4—Request for Work Experience Verification

I, _____, am applying for the Certified in Risk and Information Systems Control (CRISC)
(Applicant Printed Name)

certification. As such, my work experience in identifying, assessing, mitigating and responding to risk, and monitoring and reporting on risk and control must be independently verified by individuals knowledgeable of my work experience (current or previous employer). The individual verifying the work experience must be an independent verifier and not of any relation to the applicant nor can the applicant verify his/her own work. If I currently or once worked as an independent consultant, I can use a knowledgeable client or colleague to perform this role.

Please verify my IT risk and/or IS control-related experience as noted on my attached application form, and as described by the CRISC job practice domains and task statements (see page V-2). Please return the completed form to me for my submission to ISACA. If you have any questions concerning this form, please direct them to *support.isaca.org* or call +1.847.660.5660. Thank you.

 Applicant Signature Date

Section 5—Verification of Work Experience

Verifier Name: _____
Last/Family Name First/Given Name Middle Initial

Professional Title: _____

Company Name _____

Address _____
Street

City State/Province/Country Postal Code

Verifier E-mail: _____ Verifier Telephone Number: _____

I am attesting to the employment experience listed in Section 1—Employment History.
 Enter box number (Box 1, Box 2, etc) or employer (company) name.
 List all that apply to this verification. _____

1. I have functioned in a supervisory or other related position to the applicant and can verify his/her work experience. Yes No N/A
(Section 1 of the application)
 If no, identify why you are able to verify. _____
2. I can attest to the duration of the applicant’s work experience on this application with my organization. Yes No N/A
 If no, I attest to experience from _____ to _____.
3. I can attest to the duration of the applicant’s work experience on this application prior to his/her affiliation with my organization. Yes No N/A
4. I can attest that the tasks performed by the applicant, **as checked on the verification form page V-2**, are correct to the best of my knowledge. Yes No
5. I can attest to the fact that the applicant is competent in performing the tasks **as checked on the verification form page V-2**. Yes No
6. Is there any reason you believe this applicant **SHOULD NOT** be Certified in Risk and Information Systems Control by ISACA? Yes No

 Verifier Signature Date

Verification of Work Experience Form (page 2 of 2)

Applicant Name _____ ISACA ID# _____
Last/Family Name First/Given Name Middle Initial

Verifier Name _____

CRISC job practice domains and task statements

Applicants are required to checkmark (☑ or ☒) in each box the tasks they performed to be confirmed by the verifier. For each task checked off, the corresponding domain should be referenced in Section 1—Employment History.

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.

- 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 enterprisewide 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.

- 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.

- 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.

- 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.



Telephone: +1.847.253.1545
Fax: +1.847.253.1443
Email: application@isaca.org
Web site: www.isaca.org