ISACA Certification Exam Candidate Guide

Version 07.24

Table of Contents

Candidate Guide Overview

Review this guide thoroughly, it contains important details ISACA Exam Candidates need to know before exam day administration including scheduling information, exam eligibility and exam day rules.

This guide provides candidates with everything required to prepare for and take an ISACA certification exam and is separated into four (4) major sections outlined below.

- Certified Information Systems Auditor (CISA)
- Certified in Risk and Information Systems Control (CRISC)
- Certified Information Security Manager (CISM)
- Certified in Governance of Enterprise IT (CGEIT)
- Certified Data Privacy Solutions Engineer (CDPSE)

Section I: Introduction

1.1 - ISACA Overview and Code of Ethics

ISACA is a pace-setting, global association helping individuals and enterprises achieve the positive potential of technology.

ISACA equips professionals with the knowledge, credentials, education and community to advance their careers and transform their organizations.

ISACA leverages the expertise of its 460,000 engaged professionals in information and cybersecurity, governance, assurance, risk and innovation, as well as its enterprise performance subsidiary, CMMI® Institute, to help advance innovation through technology.

ISACA has a presence in 188 countries, including more than 220 chapters worldwide and offices in both the United States and China.

ISACA Products and Services

Membership

Being an ISACA member gives you access to exclusive member benefits including savings on ISACA products like Certification Exams, Conferences and Exam Prep materials.

Resources

Explore the latest research, guidance and expert thinking on standards, best practices and emerging trends.

Training

ISACA's globally respected training and certification programs inspire confidence that enables innovation in the workplace and career progression.

COBIT 2019®

ISACA's legacy framework for customizing and right-sizing enterprise governance of information and technology.

Certificate Programs

- COBIT Certificates
- IT Risk Fundamentals
- Certificate of Cloud Auditing Knowledge
- Cybersecurity Audit

Certification Programs

Validate your experience and know-how in IT audit, security and control. Boost your career and salary potential.

Propel your career forward in enterprise IS/IT risk management and control. Boost your career and pay.

Propel your career to senior management roles. Contribute to your enterprise from a strategic standpoint.

Validate your expertise in strategic enterprise governance. Gain visibility at the executive level.

Designed to assess a privacy professional's ability to implement privacy and design.

See how performance-based credentials boost skills and drive career success.

Take the fast track to the forefront of emerging technology understanding and ability.

Code of Ethics

ISACA sets forth a Code of Professional Ethics to guide the professional and personal conduct of its members and/or certification holders.

- Members and those certified are required to abide by ISACA's Code of Professional Ethics.
- Failure to comply can result in an investigation and disciplinary measures including but not limited to exam score nullification or certification revocation.

1.2 - ISACA Certification Program Summary

The information below provides a summary of the five ISACA certifications addressed in this guide.

	CISA Certified Information Systems Auditor An ISACA® Certification	CRISC Certified in Risk and Information Systems Control An ISACA® Certification	CISM Certified Information Security Manager An ISACA® Certification	CGEIT Certified in the Governance of Enterprise IT An ISACA® Certification	CDPSE Certified Data Privacy Solutions Engineer An ISACA® Certification
Description	Designed for IT/IS auditors, control, assurance and information security professionals.	Designed for those experienced in the management of IT risk and the design, implementation, monitoring and maintenance of IS controls.	Designed for those who manage, design, oversee and assess an enterprise's information security function.	Recognizes a wide range of professionals for their knowledge and application of enterprise IT governance principles and practices.	Designed for those experienced in the governance, architecture, and lifecycle of data privacy at a technical level.
Experience Required	Five (5) or more years of experience in IS/IT audit, control, assurance, or security. Experience waivers are available for a maximum of three (3) years.	Three (3) or more years of experience in IT risk management and IS control. No experience waivers or substitutions	Five (5) or more years of experience in information security management. Experience waivers are available for a maximum of two (2) years.	Five (5) or more years of experience in an advisory or oversight role supporting the governance of the IT-related contribution to an enterprise. No experience waivers or substitutions.	Three (3) or more years of experience in data privacy governance, privacy architecture, and/or data lifecycle work. No experience waivers or substitutions.
Domain (%)	**Domain 1** - Information System Auditing Process (18%) **Domain 2** - Governance and Management of IT (18%) **Domain 3** – Information Systems Acquisition, Development and implementation (12%) **Domain 4** - Information Systems Operation and Business Resilience (26%) **Domain 5** – Protection of Information Assets (26%)	**Domain 1** – Governance (26%) **Domain 2** – IT Risk Assessment (20%) **Domain 3** – Risk Response and Reporting (32%) **Domain 4** – Information Technology and Security (22%)	**Domain 1** – Information Security Governance (17%) **Domain 2** – Information Security Risk Management (20%) **Domain 3** – Information Security Program (33%) **Domain 4** – Incident Management (30%)	**Domain 1** – Governance of Enterprise IT (40%) **Domain 2** – IT Resources (15%) **Domain 3** – Benefits Realization (26%) **Domain 4** – Risk Optimization (19%)	**Domain 1** – Privacy Governance (34%) **Domain 2** – Privacy Architecture (36%) **Domain 3** – Data Lifecycle (30%)
Exam Languages	Chinese Simplified English French German Japanese Korean Spanish	Chinese Simplified English Spanish Korean	Chinese Simplified English Japanese Spanish	Chinese Simplified English	Chinese Simplified English Spanish German
Exam Length	4 hours (240 minutes), 150 multiple choice questions	4 hours (240 minutes), 150 multiple choice questions	4 hours (240 minutes), 150 multiple choice questions	4 hours (240 minutes), 150 multiple choice questions	3.5 hours (210 minutes), 120 multiple choice questions

Exam Fees

Exam registration fees are based on membership status at the time of exam registration.

- ISACA Member: US $575
- ISACA Nonmember: US $760

Exam registration fees are non-refundable and non-transferrable.

Resources

Below are some useful links and resources to help exam candidates learn more about ISACA Certification exams.

CISA Certification

- CISA Exam Content Outline
- Prepare for the CISA Exam
- CISA Exam Information
- CISA Application Requirements
- CISA Maintenance Requirements

CRISC Certification

- CRISC Exam Content Outline
- Prepare for the CRISC Exam
- CRISC Exam Information
- CRISC Application Requirements
- CRISC Maintenance Requirements

CISM Certification

- CISM Exam Content Outline
- Prepare for the CISM Exam
- CISM Exam Information
- CISM Application Requirements
- CISM Maintenance Requirements

CGEIT Certification

- CGEIT Exam Content Outline
- Prepare for the CGEIT Exam
- CGEIT Exam Information
- CGEIT Application Requirements
- CGEIT Maintenance Requirements

CDPSE Certification

- CDPSE Exam Content Outline
- Prepare for the CDPSE Exam
- CDPSE Exam Information
- CDPSE Application Requirements
- CDPSE Maintenance Requirements

Section II: Exam Registration and Scheduling

2.1 - Before You Register

ISACA certification exams are computer-based and administered at authorized PSI testing centers globally or as remotely proctored exams. Exam registration is continuous, meaning, candidates can register any time, no restrictions. Candidates can schedule a testing appointment as early as 48 hours after payment of exam registration fees.

Upon registration, exam candidates have a twelve (12) month eligibility period to take their exam. This means that from the date you register, you have 12 months (365 days) to take your exam. It is important to note that the exam registration fee must be paid in full before an exam candidate can schedule and take an exam.

If you need additional time to take the exam, you can purchase a 6-month exam extension for US $75. The option to extend the exam eligibility will display on your dashboard 90 days prior to the expiration of your eligibility. When an exam is scheduled, the exam must be cancelled at least 48 hours prior to the exam date to extend the eligibility. There is a maximum of two extensions on an exam.

Please be aware that the exam eligibility and registration fees will be forfeited in the event the candidate does not take the exam during the 12-month eligibility period if the testing appointment is missed or if the candidate is more than 15 minutes late for a testing appointment.

2.2 - Registering for the Exam

Exam registration must be completed online by following the steps below:

Step	Action
1.	Select your certification exam: CISA | CRISC | CISM | CGEIT | CDPSE
2.	Log-in or create an account. Note: If you are creating an account, please ensure your name is the same as what appears on your government-issued identification that you will present on exam day. See the Exam Day Rules section in this document for acceptable forms of ID. Before you register for the exam, it is important to verify there is a PSI test site with availability near you or have a compatible device for remote testing. To test your device, complete this compatibility check. If you are using a company device to take your exam, you may need your IT department's assistance or approval.
3.	Complete the registration process

Please note, during the exam registration process you will be required to accept ISACA's Terms of Use, section 16. Exams, including the conditions set forth in this Candidate Guide covering exam administration, certification rules, and the release of test results.

For step-by-step instructions on completing your online registration, please refer to the How to Register Guide.

Candidates cannot schedule a testing appointment until exam registration fees are paid in full. Exam fees are **non-refundable** and **non-transferrable.**

Registration Acknowledgement

You will receive a **Notification to Schedule** email within one (1) business day following registration and payment of the exam.

The Notification to Schedule email provides information on scheduling your exam appointment.

Registering for the Exam with Special Accommodations

Special testing accommodations must be requested during the registration process and approved by ISACA before scheduling the exam.

To request special testing accommodations please follow the steps below:

Step	Action
1.	During the exam registration process, make sure to *check* the special accommodation requirement field.
2.	Print the Special Accommodation Request Form.
3.	Complete the ISACA Special Accommodation Request Form. ***Note: Form must be completed by you and your health care professional.***
4.	Submit form to ISACA at support.isaca.org.

Special accommodation requests will not be considered until exam registration fees are paid in full. All requests must be submitted to ISACA *no later than 4 weeks* prior to your preferred exam date and are only valid for that one exam administration.

Registration Changes

There are three common registration changes that candidates request. Refer to the table below.

Type of Change	Steps
Name	⚠ The name on your ISACA account must match the name on the ID used to check-in for your exam. 1. Log-in at **www.isaca.org/myisaca**. 2. Click on the red **MY ISACA PROFILE** button. 3. Make the necessary changes. 4. Click **Save.**
Exam Language	1. Log-in at **https://www.isaca.org/myisaca/certifications**. 2. Click the "**Re-Schedule or Cancel Exam**" link to proceed to PSI's scheduling page 3. Follow the on-screen instructions to schedule your testing appointment. The Scheduling Guide is available to help you schedule and reschedule. ***Note: If you need to change your exam language, you also must reschedule the testing appointment. See Rescheduling an Exam for details.***
Exam Type	Contact ISACA Support immediately at support.isaca.org.

⚠ All change requests must be completed a minimum of 48 hours prior to your scheduled testing appointment.

2.3 - Scheduling the Exam Appointment

Eligibility

Exam eligibility is required to schedule and take an exam. Eligibility is established at the time of exam registration and is good for twelve (12) months (365 days).

Exam registration and payment are required before you can schedule and take an exam**.**
Exam fees are non-refundable and non-transferable.

You will forfeit your fees if you do not schedule and take the exam during your twelve-month eligibility period. **No eligibility extensions are allowed.**

Exam Scheduling

There are 5 key steps to schedule an exam appointment. Please note that payment is required before you can schedule an exam.

Step	Action
1.	Log-in to your **ISACA account**
2.	Click **Certification & CPE Management**
3.	Click **Schedule Your Exam** or **Visit Exam Website,** you will be taken to the PSI dashboard to schedule your exam.
4.	On the PSI dashboard, click **Schedule Exam.**
5.	Follow the step by step instructions in the **Scheduling Guide.**

You will receive a scheduling confirmation email from no-reply@psiexams.com confirming your exam appointment. Please view the **Scheduling Guide** for additional scheduling assistance.

Please note, exam appointments are only available 90 days in advance. If you do not see your exam site or date available more than 90 days in advance, please check back when it is closer to your desired exam date.

If you still do not see your desired exam site or date available, please verify that your exam eligibility has not expired by logging into your **ISACA Account**, and clicking the Certification & CPE Management tab.

Rescheduling an Exam

You can reschedule your exam anytime, without penalty, during your eligibility period if done a minimum of 48 hours prior to your scheduled testing appointment.

If you are within 48 hours of your scheduled testing appointment, you must take the exam or forfeit the registration fee. To reschedule an appointment: Log-in into your **ISACA Account** and follow the rescheduling steps in the **Scheduling Guide**

Emergency Closing

Severe weather or an emergency could require canceling scheduled exams. If this occurs, PSI will attempt to contact you by phone or email; however, ISACA suggests that you check for test center closures by visiting www.psiexams.com. If the site is closed, the exam will be rescheduled at no additional charge.

Section III - Exam Preparation

The Exam Preparation section covers the processes to get ready for the exam, the exam day rules and how the exam is administered.

3.1 - Getting Ready for the Exam

Exam Preparation

ISACA offers a variety of **exam preparation** resources including group training, self-paced training and study resources in various languages to help you prepare for your certification exam.

Exam Questions

Exam questions are developed with the intent of measuring and testing practical knowledge and the application of general concepts and standards. All questions are designed with one best answer.

- Every question has a stem (question) and four options (answer choices).
- Choose the correct or best answer from the options.
- The stem may be in the form of a question or incomplete statement.

In some instances, a scenario may also be included. These questions normally include a description of a situation and require you to answer two or more questions based on the information provided.

To learn more about the types of exam questions and how they are developed, review our **Item Writing Requirements and Resources**.

Exam Tips

- Read each question carefully. An exam question may require you to choose the appropriate answer based on a qualifier, such as MOST likely or BEST.
- Read the question carefully, eliminate known incorrect answers and then make the best choice possible.
- A tutorial of the exam taking experience will be provided after logging onto the testing station and prior to the start of the exam. Pay close attention to the tutorial so as not to miss important information.
- All questions should be answered.
- There are no penalties for incorrect answers. Grades are based solely on the total number of questions answered correctly, so do not leave any questions blank.
- Budget your time. Pace yourself to complete the entire exam. You have 4 hours to complete the CISA/CRISC/CISM/CGEIT exams, and 3.5 hours to complete the CDPSE exam.

Exams scheduled at an in-person Exam Center

If your exam is scheduled for an Exam Center, make sure you are prepared before the day of the exam by doing the following:

- Locate the test center address and confirm the start time.
- Map out your route to the testing center.
- Plan to arrive at least 30 minutes prior to the exam start time.
- Plan to store your personal belongings.

*See the **Exam Day Rules** for more information.

Remotely Proctored Exams

For additional information about remotely proctored exams, download the Remote Proctoring Guide. To test your device, complete this compatibility check prior to your exam day.

If you are using a company device to take your exam, you may need your IT department's assistance or approval to download the secure browser.

*See the **Exam Day Rules** for more information.

Identification Requirements

To enter the testing center or check-in for your online exam, you must present an acceptable form of identification (ID). An acceptable form of ID must be a current, valid, and original government-issued ID that contains:

- Candidate's name (as it appears on the Notification to Schedule email from ISACA). *Please note, the first and last name shown on your ID must match the name with which you registered for the exam, or you may not be permitted entry to your exam. Middle names are not required for registration.*
- Candidate's signature *(Driver's Licenses issued in Japan without a signature will be accepted.)*
- Candidate's photograph

All information must be demonstrated by a single form of ID (cannot be a copy or handwritten).

Any candidate who does not provide an acceptable form of ID will not be allowed to sit for the exam and will forfeit their registration fee.

Acceptable Forms of Identification

Acceptable forms of identification include:

- Driver's license
- State identity card (non-driver's license)
- Passport
- Passport card
- Green card
- Alien registration
- Permanent resident card
- National identification card

The testing center reserves the right to ask for additional forms of identification for verification purposes. If there is any doubt surrounding your identity, you will be turned away from the test and ISACA will be notified. This will be considered a no-show and you forfeit your exam fees. To take the exam in the future, you will be required to re-register and pay the exam fee again.

3.2 - Exam Day Rules

The exam rules provide guidelines of what is acceptable during the exam. The exam rules apply for tests administered at PSI Test Center locations and Remotely Proctored Exams. Upon registering for any ISACA exam, candidates must accept the Terms of Use, section 16. Exams. Per these Terms, ISACA has the right to nullify exam scores if any of these unacceptable behaviors are identified.

Prohibited Items

Your workspace must be completely cleared of all other items and materials during your exam. You will be required to face toward the screen for the duration of your exam so the proctors can properly monitor the exam session.

You are prohibited from having the following items with you during your exam:

- Reference materials, study materials, paper, notes, notepads, language dictionaries, or other aids
- Calculators
- Multiple monitors
- Any type of communication, surveillance or recording devices including but not limited to:
  - Mobile phones (allowed with remotely proctored exams for mirror check), electronic devices, or recording devices
  - Tablets
  - Smart watches or glasses
  - Headphones / earbuds
- Baggage of any kind including handbags, purses, or briefcases
- Weapons
- Tobacco products or vaping
- Food or beverages (this includes water, and applies to both on-site and remotely proctored exams)
- Visitors

If exam candidates are viewed with any such communication, surveillance or recording devices during the exam administration, their exam will be voided, and they will be asked to immediately leave the exam site if applicable. Candidates are not permitted to take screenshots or photos of any portion of the exam, including the exam results screen.

Storing Personal Items

Plan to store your personal items brought to the testing center in a locker or other designated area. You will not be able to access personal items until the exam is complete and submitted.

Unacceptable behavior

Per the Terms of Use, section 16. Exams, the following activities are prohibited.

- Creating a disturbance.
- Giving or receiving assistance during the exam; using notes, papers, or other aids; use of unauthorized study materials
- Talking, reading the questions out loud, or moving your lips while reading silently
- Copy, photograph, record, memorize or otherwise attempt to retain or recreate any Exam content, or assisting anyone to retain recreate or reconstruct Exam content for any purpose
- Attempting to take the exam for someone else or having someone else take the exam for you.
- Possession of communication, surveillance or recording device, including but not limited to cell phones, tablets, smart glasses, smart watches, mobile devices, etc., during the exam administration.
- Attempting to sell, license, distribute, exchange, give away, share, comment on, disclose or discuss, either directly or indirectly, any exam content to any person or entity before, during or after the Exam verbally, in writing, or through any other method of communication including but not limited to the Internet, email, or through any online forum.
- Leaving the testing area without authorization. (These individuals will not be allowed to return to the testing room). Two breaks, each no longer than ten minutes, are permitted with permission of your proctor. Your exam will be paused, but the timer will not stop during your approved breaks.
- Accessing items stored in the personal belongings area before the completion of the exam.

Personal Hardship Guidelines

If you fail to arrive for a testing appointment due to a personal hardship you may be able to reschedule without forfeiting your exam registration fee.

Step	Action
1.	Contact PSI* no later than 72 hours following the scheduled appointment.
2.	Provide documentation to PSI to confirm the reason for absence.

***PSI Contact Info:**

Step	Action
1.	Visit https://www.psionline.com/test-takers/candidate-support-numbers/
2.	Enter "ISACA" in the Search field.
3.	Review and choose from the list of available contact numbers.

Personal Hardship Examples	Documentation Required
Personal Illness	Doctor's note, emergency room admittance, etc. • Must be signed by a licensed doctor and include the date of medical visit. • Must include contact information for the licensed doctor. • Does not need to give details of the illness or emergency, but the doctor should indicate that the candidate should not test.
Death of an immediate family member including: • Spouse • Child/dependent • Parent • Grandparent • Sibling	Must include the date of death and deceased name and relationship to the deceased.
Traffic Accidents	Police report, receipt from the mechanic or towing company which must include the date and contact information.

If the request is denied, you are required to register again and pay the full exam registration fee.

Leaving the Testing Area

You must gain authorization from the test proctor to leave the testing center or in the case of online remotely proctored exams, to leave your designated testing area. Leaving your testing center or testing area without authorization may result in your exam being terminated. Two breaks are permitted with permission of your proctor. Your exam will be paused, but the timer will not stop during your approved breaks.

Reason for leaving:	Directions:
An emergency	• The exam will be paused temporarily. • Once it is confirmed as an emergency, the test will end.
To use the facilities	• You will be required to check out and check back in. • The exam time will not stop, and no extra time will be permitted. • Each of your two breaks must be 10 minutes or less.

Consequences

If you violate the Terms of Use or Exam Day Rules or engage in any kind of misconduct you will be subject to the following:

- Dismissal or disqualification
- Voiding of exam
- Revocation of ISACA membership and any certifications currently held
- Banned from taking any ISACA exam

3.3 - Exam Administration

The PSI testing location is either a testing center or online remoted proctored.

PSI Testing Center

Your exam may be administered in a room with other test takers. Please note that some noise should be expected and is considered normal.

Here is a video of the PSI Test Center Experience.

Online Remote Proctoring

ISACA also offers the ability to take exams at home via online remote proctoring. Please review the **Remote Proctoring Guide** prior to taking an exam using this delivery modality.

ISACA will require a mirror check for each exam following the room scan. The purpose of the mirror check is to show the proctor the blind spots not captured during the room scan using a built-in webcam. A portable mirror or mobile phone may be used to complete the mirror check. During the mirror check, you will be required to hold the mirror up to the webcam and display the monitor/laptop screen, keyboard and all four edges of the monitor/laptop screen. If using a mobile phone, it will need to be placed out of reach in the room designated for testing after the mirror check is completed.

Here is a video of the PSI Online Remote Proctoring Experience.

Section IV - After the Exam

The After the Exam section covers the exam scoring and applying for certification.

4.1 - Exam Scoring

Receiving Your Score

You will be able to view your preliminary passing status on screen immediately following the completion of your exam. You are not permitted to take screenshots or photos of any portion of the exam, including the exam results screen. Your official score will be emailed and available online within 10 working days. If you have passed your exam, you will receive details on how to apply for certification.

1. Email notification: sent to the email address listed on your profile.
2. Online results: available on MyISACA > Certifications & CPE Management page.
3. Exam scores will not be provided by telephone or fax.
4. **Question-level results cannot be provided.**

Scoring Criteria

Candidate scores are reported as a scaled score. A scaled score is a conversion of a candidate's raw score on an exam to a common scale. The purpose of a scaled score is to ensure that a standard way of reporting outcomes is used across disparate versions of the exam so that different versions are comparable and fair. ISACA uses and reports scores on a common scale from 200 to 800. ISACA exams are comprised of scored items as well as pre-test items. Pre-test items are not used to calculate your exam score. Review the points below to identify the lowest, passing, and perfect scores.

- A score of 800 represents a perfect score with all questions answered correctly.
- A score of 200 represents the lowest score possible and signifies only a small number of questions were answered correctly.
- You must receive a score of 450 or higher to pass the exam which represents the minimum standard of knowledge.
- Domain level results are provided for informational purposes only. Exam scores are based on the total number of exam items answered correctly, regardless of domain. Domain percentages indicate the portion of the exam that reflects that domain content and are not used to calculate exam scores.
- A candidate receiving a passing score can then apply for certification if all other requirements are met (see section How to become Certified for more details).

Requests for Rescoring

While we are confident in the integrity and validity of our scoring procedures, you may request a rescore if you do not pass the exam. Rescores are performed by PSI.

You must submit a rescore request in writing through our support page within 30 days following the release of the exam results.

- Requests for a rescore after 30 days will not be processed.
- All requests must include a candidate's name, ISACA ID number and mailing address.
- A fee of US $75 must accompany each request.

4.2 - Retake Policy

To protect the integrity of ISACA's certification exams, ISACA has implemented the following retake policy:

1. Individuals have 4 attempts within a rolling twelve-month period to pass the exam. Those that do not pass on their first attempt are allowed to retake the exam a total of 3 more times within 12 months from the date of the first attempt. **Please note that candidates must pay the registration fee in full for each exam attempt.**

   To illustrate:

   After taking and not passing the exam (attempt 1):

   - Retake 1 (attempt 2): Customers must wait 30 days from the date of the first attempt
   - Retake 2 (attempt 3): Customers must wait 90 days after the date of the second attempt
   - Retake 3 (attempt 4): Customers must wait 90 days after the date of the third attempt

2. Individuals who pass the exam are restricted from taking the same exam within the application time period of 5 years.
3. Certification holders are restricted from taking the same certification exam while they are certified.

4.3 - Post Exam Feedback

You will have the opportunity to provide feedback after completing the exam via a post-exam survey. Your feedback is used to improve the testing experience and the quality of the exam questions.

Concerns about Exam Administration

You can provide comments and concerns about the examination administration, including exam day issues, site conditions or the content of the exam by contacting ISACA at support.isaca.org within 48 hours of the conclusion of the test.

Step	Action
1.	Contact ISACA support.
2.	Provide the following information in your comments: • ISACA ID number • Testing center location • Date and time tested • Any relevant details on the specific issue
3.	ISACA will review comments regarding exam day issues and site concerns prior to the release of the official score report.

ISACA does not reissue scores based on question updates. Our subject matter experts use these comments to improve future examinations.

4.4 - Certification

How to become Certified

Taking and passing an ISACA certification exam is just the first step in becoming certified. To become certified, an individual must first meet the following requirements:

Step	Action
1.	Successfully pass the Certification Exam.
2.	Pay the $50 application processing fee.
3.	Submit an application to demonstrate the experience requirements.
4.	Adhere to the Code of Professional Ethics.
5.	Adhere to the Continuing Professional Education Policy.

Candidates have (5) five years from passing the exam to apply for certification.

Additional resources are included below for more information about becoming certified.

1. Pass the Examination: CISA | CISM | CGEIT | CRISC | CDPSE
2. Pay the $50 Application Processing Fee: CISA | CISM | CGEIT | CRISC | CDPSE
3. Submit the Application for Certification: CISA | CISM | CGEIT | CRISC | CDPSE
4. Adhere to ISACA's Code of Professional Ethics, Terms of Use, and Privacy Policy
5. Adhere to the Continuing Professional Education (CPE) Policy: CISA | CISM | CGEIT | CRISC |CDPSE
6. Compliance with the Information Systems Auditing Standards (CISA only)

Why certify?

ISACA certifications are globally accepted and recognized. They combine the achievement of passing an exam with credit for your work and educational experience, giving you the credibility you need to move ahead in your career. Certification proves to employers that you have what it takes to add value to their enterprise. In fact, many organizations and governmental agencies around the world require or recognize ISACA's certifications.

Independent studies consistently rate ISACA's designations among the highest paying IT and impactful certifications that an IT professional can earn. Earning and maintaining an ISACA certification:

- Boosts your earning potential.
- Counts in the hiring process.
- Enhances your professional credibility and recognition.

ISO/IEC 17024:2012 Compliant

- The American National Standards Institute (ANSI) has accredited the CISA, CRISC, CISM and CGEIT certifications under ISO/IEC 17024:2012, General Requirements for Bodies Operating Certification Systems of Persons.
- Accreditation by ANSI signifies that ISACA's procedures meet ANSI's essential requirements for openness, balance, consensus, and due process.
- With this accreditation, ISACA anticipates that significant opportunities for CISAs, CRISCs, CISMs and CGEITs will continue to present themselves around the world.

ANSI Accredited Program

PERSONNEL CERTIFICATION #0694

ISO/IEC 17024

CISA, CISM, CGEIT and CRISC Program Accreditation

Renewed Under ISO/IEC 17024:2012

- ANSI is a private, nonprofit organization that accredits other organizations to serve as third-party product, system, and personnel certifiers.
- ISO/IEC 17024 specifies the requirements to be followed by organizations certifying individuals against specific requirements.

ANSI describes ISO/IEC 17024 as "expected to play a prominent role in facilitating global standardization of the certification community, increasing mobility among countries, enhancing public safety and protecting consumers."

APPENDIX

Appendix A

CISA exam content outline

Appendix B

CRISC exam content outline

Appendix C

CISM exam content outline

Appendix D

CGEIT exam content outline

Appendix E

CDPSE exam content outline

Appendix A

CISA Examination Content Outline

(Effective August 2024)

1	**Information System Auditing Process**
A	Planning
1	IS Audit Standards, Guidelines, Functions, and Codes of Ethics
2	Types of Audits, Assessments, and Reviews
3	Risk-Based Audit Planning
4	Types of Controls and Considerations
B	Execution
1	Audit Project Management
2	Audit Testing and Sampling Methodology
3	Audit Evidence Collection Techniques
4	Audit Data Analytics (including audit algorithms)
5	Reporting and Communication Techniques
6	Quality Assurance and Improvement of Audit Process
2	**Governance and Management of IT**
A	IT Governance
1	Laws, Regulations, and Industry Standards
2	Organizational Structure, IT Governance, and IT Strategy
3	IT Policies, Standards, Procedures and Practices
4	Enterprise Architecture (EA) and Considerations
5	Enterprise Risk Management (ERM)
6	Privacy Program and Principles
7	Data Governance and Classification
B	IT Management
1	IT Resource Management
2	IT Vendor Management
3	IT Performance Monitoring and Reporting
4	Quality Assurance and Quality Management of IT
3	**Information Systems Acquisition, Development, and Implementation**
A	Information Systems Acquisition and Development
1	Project Governance and Management
2	Business Case and Feasibility Analysis
3	System Development Methodologies
4	Control Identification and Design
B	Information Systems Implementation
1	System Readiness and Implementation Testing
2	Implementation Configuration and Release Management
3	System Migration, Infrastructure Deployment, and Data Conversion
4	Post-Implementation Review

4	**Information Systems Operations and Business Resilience**
A	Information Systems Operations
1	IT Components
2	IT Asset Management
3	Job Scheduling and Production Process Automation
4	System Interfaces
5	Shadow IT and End-User Computing (EUC)
6	Systems Availability and Capacity Management
7	Problem and Incident Management
8	IT Change, Configuration, and Patch Management
9	Operational Log Management
10	IT Service Level Management
11	Database Management
B	Business Resilience
1	Business Impact Analysis (BIA)
2	System and Operational Resilience
3	Data Backup, Storage, and Restoration
4	Business Continuity Plan (BCP)
5	Disaster Recovery Plans (DRP)
5	**Protection of Information Assets**
A	Information Asset Security and Control
1	Information Asset Security Policies, Frameworks, Standards, and Guidelines
2	Physical and Environmental Controls
3	Identity and Access Management
4	Network and End-Point Security
5	Data Loss Prevention (DLP)
6	Data Encryption
7	Public Key Infrastructure (PKI)
8	Cloud and Virtualized Environments
9	Mobile, Wireless, and Internet-of-Things (IoT) Devices
B	Security Event Management
1	Security Awareness Training and Programs
2	Information System Attack Methods and Techniques
3	Security Testing Tools and Techniques
4	Security Monitoring Logs, Tools, and Techniques
5	Security Incident Response Management
6	Evidence Collection and Forensics

Supporting Tasks

1. Plan an audit to determine whether information systems are protected, controlled, and provide value to the organization.
2. Conduct audits in accordance with IS audit standards and a risk based IS audit strategy.
3. Apply project management methodologies to the audit process.
4. Communicate and collect feedback on audit progress, findings, results, and recommendations with stakeholders.
5. Conduct post-audit follow up to evaluate whether identified risk has been sufficiently addressed.
6. Utilize data analytics tools to enhance audit processes.
7. Evaluate the role and/or impact of automatization and/or decision-making systems for an organization.
8. Evaluate audit processes as part of quality assurance and improvement programs.
9. Evaluate the IT strategy for alignment with the organization's strategies and objectives.
10. Evaluate the effectiveness of IT governance structure and IT organizational structure.
11. Evaluate the organization's management of IT policies and practices, including compliance with legal and regulatory requirements.
12. Evaluate IT resource and project management for alignment with the organization's strategies and objectives.
13. Evaluate the organization's enterprise risk management (ERM) program.
14. Determine whether the organization has defined ownership of IT risk, controls, and standards.
15. Evaluate the monitoring and reporting of IT key performance indicators (KPIs) and IT key risk indicators (KRIs).
16. Evaluate the organization's ability to continue business operations.
17. Evaluate the organization's storage, backup, and restoration policies and processes.
18. Evaluate whether the business cases related to information systems meet business objectives.
19. Evaluate whether IT vendor selection and contract management processes meet business, legal, and regulatory requirements.
20. Evaluate supply chains for IT risk factors and integrity issues.
21. Evaluate controls at all stages of the information systems development life cycle.
22. Evaluate the readiness of information systems for implementation and migration into production.
23. Conduct post-implementation reviews of systems to determine whether project deliverables, controls, and requirements are met.
24. Evaluate whether effective processes are in place to support end users.
25. Evaluate whether IT service management practices align with organizational requirements.
26. Conduct periodic review of information systems and enterprise architecture (EA) to determine alignment with organizational objectives.
27. Evaluate whether IT operations and maintenance practices support the organization's objectives.
28. Evaluate the organization's database management practices.
29. Evaluate the organization's data governance program.
30. Evaluate the organization's privacy program.
31. Evaluate data classification practices for alignment with the organization's data governance program, privacy program, and applicable external requirements.
32. Evaluate the organization's problem and incident management program.
33. Evaluate the organization's change, configuration, release, and patch management programs.
34. Evaluate the organization's log management program.
35. Evaluate the organization's policies and practices related to asset life cycle management.

36. Evaluate risk associated with shadow IT and end-user computing (EUC) to determine effectiveness of compensating controls.
37. Evaluate the organization's information security program.
38. Evaluate the organization's threat and vulnerability management program.
39. Utilize technical security testing to identify potential vulnerabilities.
40. Evaluate logical, physical, and environmental controls to verify the confidentiality, integrity, and availability of information assets.
41. Evaluate the organization's security awareness training program.
42. Provide guidance to the organization in order to improve the quality and control of information systems.
43. Evaluate potential opportunities and risks associated with emerging technologies, regulations, and industry practices.

Appendix B

CRISC Examination Content Outline
(Effective 2021)

1	**Governance**
A	Organizational Governance
1A1	Organizational Strategy, Goals and Objectives
1A2	Organizational Structure, Roles, and Responsibilities
1A3	Organizational Culture
1A4	Policies and Standards
1A5	Business Processes
1A6	Organizational Assets
B	Risk Governance
1B1	Enterprise Risk Management
1B2	Three Lines of Defense
1B3	Risk Profile
1B4	Risk Appetite and Risk Tolerance
1B5	Legal, Regulatory, and Contractual Requirements
1B6	Professional Ethics of Risk Management
2	**IT Risk Assessment**
A	IT Risk Identification
2A1	Risk Events
2A2	Threat Modeling and Threat Landscape
2A3	Vulnerability and Control Deficiency Analysis (e.g., root cause analysis, gap analysis)
2A4	Risk Scenario Development
B	IT Risk Analysis and Evaluation
2B1	Risk Assessment Concepts, Standards, and Frameworks
2B2	Risk Register
2B3	Risk Analysis Methodologies
2B4	Business Impact Analysis
2B5	Inherent and Residual Risk
3	**Risk Response and Reporting**
A	Risk Response
3A1	Risk Treatment / Risk Response Options
3A2	Risk and Control Ownership
3A3	Third-Party Risk Management
3A4	Issue, Finding, and Exception Management
3A5	Management of Emerging Risk
B	Control Design and Implementation
3B1	Control Types, Standards, and Frameworks
3B2	Control Design, Selection, and Analysis
3B3	Control Implementation
3B4	Control Testing and Effectiveness Evaluation
C	Risk Monitoring and Reporting
3C1	Risk Treatment Plans / Risk Action Plans
3C2	Data Collection, Aggregation, Analysis, and Validation
3C3	Risk and Control Monitoring Techniques

3C4	Risk and Control Reporting Techniques (e.g., heatmap, scorecards, dashboards)
3C5	Key Performance Indicators (KPIs)
3C6	Key Risk Indicators (KRIs)
3C7	Key Control Indicators (KCIs)
4	**Information Technology and Security**
A	Information Technology Principles
4A1	Enterprise Architecture
4A2	IT Operations Management
4A3	Project Management
4A4	Disaster Recovery Management (DRM)
4A5	Data Lifecycle Management
4A6	System Development Life Cycle (SDLC)
4A7	Emerging Technologies
B	Information Security Principles
4B1	Information Security Concepts, Frameworks, and Standards
4B2	Information Security Awareness Training
4B3	Business Continuity Management
4B4	Data Privacy and Data Protection Principles

Supporting Tasks

1. Collect and review existing information regarding the organization's business and IT environments.
2. Identify potential or realized impacts of IT risk to the organization's business objectives and operations.
3. Identify threats and vulnerabilities to the organization's people, processes, and technologies.
4. Develop IT risk scenarios to determine the potential impact to business objectives and operations.
5. Establish accountability by assigning and validating appropriate levels of risk and control ownership.
6. Establish and maintain the IT risk register and incorporate it into the enterprise-wide risk profile.
7. Facilitate the identification of risk appetite and risk tolerance by key stakeholders.
8. Promote a risk-aware by contributing to the development and implementation of security awareness training.
9. Conduct a risk assessment by analysing IT risk scenarios and determining their likelihood and impact.
10. Identify the current state of existing controls and evaluate their effectiveness for IT risk mitigation.
11. Review the results of risk analysis and control analysis to assess any gaps between current and desired states of the IT risk environment.
12. Facilitate the selection of recommended risk responses by key stakeholders.
13. Collaborate with risk owners on the development of risk treatment plans.
14. Collaborate with control owners on the design, implementation, and maintenance of controls.
15. Validate that risk responses have been executed according to risk treatment plans.
16. Define and establish key risk indicators (KRIs).
17. Monitor and analyze key risk indicators (KRIs).
18. Collaborate with control owners on the identification of key performance indicators (KPIs) and key control indicators (KCIs).
19. Monitor and analyze key performance indicators (KPIs) and key control indicators (KCIs).
20. Review the results of control assessments to determine the effectiveness and maturity of the control environment.
21. Conduct aggregation, analysis, and validation of risk and control data.
22. Report relevant risk and control information to applicable stakeholders to facilitate risk-based decision-making.
23. Evaluate emerging technologies and changes to the environment for threats, vulnerabilities, and opportunities.
24. Evaluate alignment of business practices with risk management and information security frameworks and standards.

Appendix C

CISM Examination Content Outline
(Effective 2022)

1	Information Security Governance (17%)
A	Enterprise Governance
1A1	Organizational Culture
1A2	Legal, Regulatory, and Contractual Requirements
1A3	Organizational Structures, Roles, and Responsibilities
B	Information Security Strategy
1B1	Information Security Strategy Development
1B2	Information Governance Frameworks and Standards
1B3	Strategic Planning (e.g., budgets, resources, business case)
2	Information Security Risk Management (20%)
A	Information Security Risk Assessment
2A1	Emerging Risk and Threat Landscape
2A2	Vulnerability and Control Deficiency Analysis
2A3	Risk Assessment and Analysis
B	Information Security Risk Response
2B1	Risk Treatment / Risk Response Options
2B2	Risk and Control Ownership
2B3	Risk Monitoring and Reporting
3	Information Security Program (33%)
A	Information Security Program Development
3A1	Information Security Program Resources (e.g., people, tools, technologies)
3A2	Information Asset Identification and Classification
3A3	Industry Standards and Frameworks for Information Security
3A4	Information Security Policies, Procedures, and Guidelines
3A5	Information Security Program Metrics
B	Information Security Program Management
3B1	Information Security Control Design and Selection
3B2	Information Security Control Implementation and Integrations
3B3	Information Security Control Testing and Evaluation
3B4	Information Security Awareness and Training
3B5	Management of External Services (e.g., providers, suppliers, third parties, fourth parties)
3B6	Information Security Program Communications and Reporting
4	Incident Management (30%)
A	Incident Management Readiness
4A1	Incident Response Plan
4A2	Business Impact Analysis (BIA)
4A3	Business Continuity Plan (BCP)
4A4	Disaster Recovery Plan (DRP)
4A5	Incident Classification/Categorization
4A6	Incident Management Training, Testing, and Evaluation

B	Incident Management Operations
4B1	Incident Management Tools and Techniques
4B2	Incident Investigation and Evaluation
4B3	Incident Containment Methods
4B4	Incident Response Communications (e.g., reporting, notification, escalation)
4B5	Incident Eradication and Recovery
4B6	Post-incident Review Practices

Supporting Tasks

1. Identify internal and external influences to the organization that impact the information security strategy.
2. Establish and/or maintain an information security strategy in alignment with organizational goals and objectives.
3. Establish and/or maintain an information security governance framework.
4. Integrate information security governance into corporate governance.
5. Establish and maintain information security policies to guide the development of standards, procedures, and guidelines.
6. Develop business cases to support investments in information security.
7. Gain ongoing commitment from senior leadership and other stakeholders to support the successful implementation of the information security strategy.
8. Define, communicate, and monitor information security responsibilities throughout the organization and lines of authority.
9. Compile and present reports to key stakeholders on the activities, trends, and overall effectiveness of the information security program.
10. Evaluate and report information security metrics to key stakeholders.
11. Establish and/or maintain the information security program in alignment with the information security strategy.
12. Align the information security program with the operational objectives of other business functions.
13. Establish and maintain information security processes and resources to execute the information security program.
14. Establish, communicate, and maintain organizational information security policies, standards, guidelines, procedures, and other documentation.
15. Establish, promote, and maintain a program for information security awareness and training.
16. Integrate information security requirements into organizational processes to maintain the organization’s security strategy.
17. Integrate information security requirements into contracts and activities of external parties.
18. Monitor external parties' adherence to established security requirements.
19. Define and monitor management and operational metrics for the information security program.
20. Establish and/or maintain a process for information asset identification and classification.
21. Identify legal, regulatory, organizational, and other applicable compliance requirements.
22. Participate in and/or oversee the risk identification, risk assessment, and risk treatment process.
23. Participate in and/or oversee the vulnerability assessment and threat analysis process.
24. Identify, recommend, or implement appropriate risk treatment and response options to manage risk to acceptable levels based on organizational risk appetite.
25. Determine whether information security controls are appropriate and effectively manage risk to an acceptable level.
26. Facilitate the integration of information risk management into business and IT processes.
27. Monitor for internal and external factors that may require reassessment of risk.
28. Report on information security risk, including noncompliance and changes in information risk, to key stakeholders to facilitate the risk management decision-making process.
29. Establish and maintain an incident response plan, in alignment with the business continuity plan and disaster recovery plan.
30. Establish and maintain an information security incident classification and categorization process.
31. Develop and implement processes to ensure the timely identification of information security incidents.
32. Establish and maintain processes to investigate and document information security incidents in accordance with legal and regulatory requirements.

33. Establish and maintain incident handling process, including containment, notification, escalation, eradication, and recovery.
34. Organize, train, equip, and assign responsibilities to incident response teams.
35. Establish and maintain incident communication plans and processes for internal and external parties.
36. Evaluate incident management plans through testing and review, including table-top exercises, checklist review, and simulation testing at planned intervals.
37. Conduct post-incident reviews to facilitate continuous improvement, including root-cause analysis, lessons learned, corrective actions, and reassessment of risk.

Appendix D

CGEIT Examination Content Outline
(Effective 2020)

1	**Governance of Enterprise IT**
A	Governance Framework
1A1	Components of a Governance Framework
1A2	Organizational Structures, Roles, and Responsibilities
1A3	Strategy Development
1A4	Legal and Regulatory Compliance
1A5	Organizational Culture
1A6	Business Ethics
B	Technology Governance
1B1	Governance Strategy Alignment with Enterprise Objectives
1B2	Strategic Planning Process
1B3	Stakeholder Analysis and Engagement
1B4	Communication and Awareness Strategy
1B5	Enterprise Architecture
1B6	Policies and Standards
C	Information Governance
1C1	Information Architecture
1C2	Information Asset Lifecycle
1C3	Information Ownership and Stewardship
1C4	Information Classification and Handling
2	**IT Resources**
A	IT Resource Planning
2A1	Sourcing Strategies
2A2	Resource Capacity Planning
2A3	Acquisition of Resources
B	IT Resource Optimization
2B1	IT Resource Lifecycle and Asset Management
2B2	Human Resource Competency Assessment and Development
2B3	Management of Contracted Services and Relationships
3	**Benefits Realization**
A	IT Performance and Oversight
3A1	Performance Management
3A2	Change Management
3A3	Governance Monitoring
3A4	Governance Reporting
3A5	Quality Assurance
3A6	Process Development and Improvement
B	Management of IT-Enabled Investments
3B1	Business Case Development and Evaluation
3B2	IT Investment management and Reporting
3B3	Performance Metrics
3B4	Benefit Evaluation Methods
4	**Risk Optimization**

A	Risk Strategy
4A1	Risk Frameworks and Standards
4A2	Enterprise Risk Management
4A3	Risk Appetite and Risk Tolerance
B	Risk Management
4B1	IT-Enabled Capabilities, Processes, and Services
4B2	Business Risk, Exposures, and Threats
4B3	Risk management Lifecycle
4B4	Risk Assessment Methods

Supporting Tasks

1. Establish the objectives for the framework for the governance of enterprise IT.
2. Establish a framework for the governance of enterprise IT.
3. Identify the internal and external requirements for the framework for the governance of enterprise IT.
4. Incorporate a strategic planning process into the framework for the governance of enterprise IT.
5. Ensure that a business case development and benefits realization process for IT-enabled investments has been established.
6. Incorporate enterprise architecture into the framework for the governance of enterprise IT.
7. Incorporate information architecture into the framework for the governance of enterprise IT.
8. Align the framework for the governance of enterprise IT with enterprise-wide shared services.
9. Incorporate comprehensive and repeatable processes and activities into the framework for the governance of enterprise IT.
10. Establish roles, responsibilities, and accountabilities for information assets and IT processes.
11. Evaluate the framework for the governance of enterprise IT and identify improvement opportunities.
12. Establish a process for the identification and remediation of issues related to the framework for the governance of enterprise IT.
13. Establish policies and standards that support IT and enterprise strategic alignment.
14. Establish policies and standards that inform decision-making with regard to IT-enabled business investments.
15. Establish communication and awareness processes to convey the value of the governance of enterprise IT.
16. Evaluate, direct, and monitor IT strategic planning processes to ensure alignment with enterprise goals.
17. Evaluate, direct, and monitor stakeholder engagement.
18. Document and communicate the IT strategic planning processes and related outputs.
19. Ensure that enterprise architecture is integrated into the IT strategic planning process.
20. Ensure that information architecture is integrated into the IT strategic planning process.
21. Incorporate a prioritization process for IT initiatives into the framework for the governance of enterprise IT.
22. Ensure that processes are in place to manage the lifecycle of IT resources and capabilities.
23. Ensure that processes are in place to govern the lifecycle of information assets.
24. Incorporate sourcing strategies into the framework for the governance of enterprise IT to ensure optimization and control.
25. Ensure the alignment of IT resource management processes with the enterprise’s resource management processes.
26. Ensure the alignment of information governance with the framework for the governance of enterprise IT.
27. Ensure that processes are in place for the assessment and development of personnel to align with business needs.
28. Ensure that IT-enabled investments are managed through their economic lifecycle.
29. Evaluate the process that assigns ownership and accountability for IT-enabled investments.
30. Ensure that IT investment management practices align with enterprise investment management practices.

31. Evaluate the benefits realization of IT-enabled investments, IT processes, and IT services.
32. Establish a performance management program for IT-enabled investments, IT processes, and IT services.
33. Ensure that improvement initiatives are based on the results derived from performance measures.
34. Ensure that comprehensive IT and information risk management programs are established.
35. Ensure that a process is in place to monitor and report on the adherence to IT and information risk management policies and standards.
36. Ensure the alignment of IT processes with the enterprise's legal and regulatory compliance objectives.
37. Ensure the alignment of IT and information risk management with the enterprise risk management framework.
38. Ensure that IT and information risk management policies and standards are developed and communicated.

Appendix E

CDPSE Examination Content Outline
(Effective 2020)

1	Privacy Governance
1A	Governance
1A1	Personal Data and Information
1A2	Privacy Laws and Standards across Jurisdictions
1A3	Privacy Documentation (e.g., Policies, Guidelines)
1A4	Legal Purpose, Consent, and Legitimate Interest
1A5	Data Subject Rights
1B	Management
1B1	Roles and Responsibilities related to Data
1B2	Privacy Training and Awareness
1B3	Vendor and Third-Party Management
1B4	Audit Process
1B5	Privacy Incident Management
1C	Risk Management
1C1	Risk Management Process
1C2	Privacy Impact Assessment (PIA)
1C3	Threats, Attacks, and Vulnerabilities related to Privacy

2	Privacy Architecture
2A	Infrastructure
2A1	Technology Stacks
2A2	Cloud-based Services
2A3	Endpoints
2A4	Remote Access
2A5	System Hardening
2B	Applications and Software
2B1	Secure Development Lifecycle (e.g., Privacy by Design)
2B2	Applications and Software Hardening
2B3	APIs and Services
2B4	Tracking Technologies
2C	Technical Privacy Controls
2C1	Communication and Transport Protocols
2C2	Encryption, Hashing, and De-identification
2C3	Key Management
2C4	Monitoring and Logging
2C5	Identity and Access Management

3	Data Lifecycle
3A	Data Purpose
3A1	Data Inventory and Classification (e.g., Tagging, Tracking, SOR)
3A2	Data Quality and Accuracy
3A3	Dataflow and Usage Diagrams
3A4	Data Use Limitation
3A5	Data Analytics (e.g., Aggregation, AI, Machine Learning, Big Data)
3B	Data Persistence
3B1	Data Minimization (e.g., De-identification, Anonymization)
3B2	Data Migration
3B3	Data Storage
3B4	Data Warehousing (e.g., Data Lake)
3B5	Data Retention and Archiving
3B6	Data Destruction

Supporting Tasks

1. Identify the internal and external requirements for the organization's privacy programs and practices.
2. Participate in the evaluation of privacy policies, programs, and policies for their alignment with legal requirements, regulatory requirements, and/or industry best practices.
3. Coordinate and/or perform privacy impact assessment (PIA) and other privacy-focused assessments.
4. Participate in the development of procedures that align with privacy policies and business needs.
5. Implement procedures that align with privacy policies.
6. Participate in the management and evaluation of contracts, service levels, and practices of vendors and other external parties.
7. Participate in the privacy incident management process.
8. Collaborate with cybersecurity personnel on the security risk assessment process to address privacy compliance and risk mitigation.
9. Collaborate with other practitioners to ensure that privacy programs and practices are followed during the design, development, and implementation of systems, applications, and infrastructure.
10. Evaluate the enterprise architecture and information architecture to ensure it supports privacy by design principles and considerations.
11. Evaluate advancements in privacy-enhancing technologies and changes in the regulatory landscape.
12. Identify, validate, and/or implement appropriate privacy and security controls according to data classification procedures.
13. Design, implement, and/or monitor processes and procedures to keep the inventory and dataflow records current.
14. Develop and/or implement a prioritization process for privacy practices.
15. Develop, monitor, and/or report performance metrics and trends related to privacy practices.
16. Report on the status and outcomes of privacy programs and practices to relevant stakeholders.
17. Participate in privacy training and promote awareness of privacy practices.
18. Identify issues requiring remediation and opportunities for process improvement.