ISACA Certification Exam Candidate Guide

Version 11.25

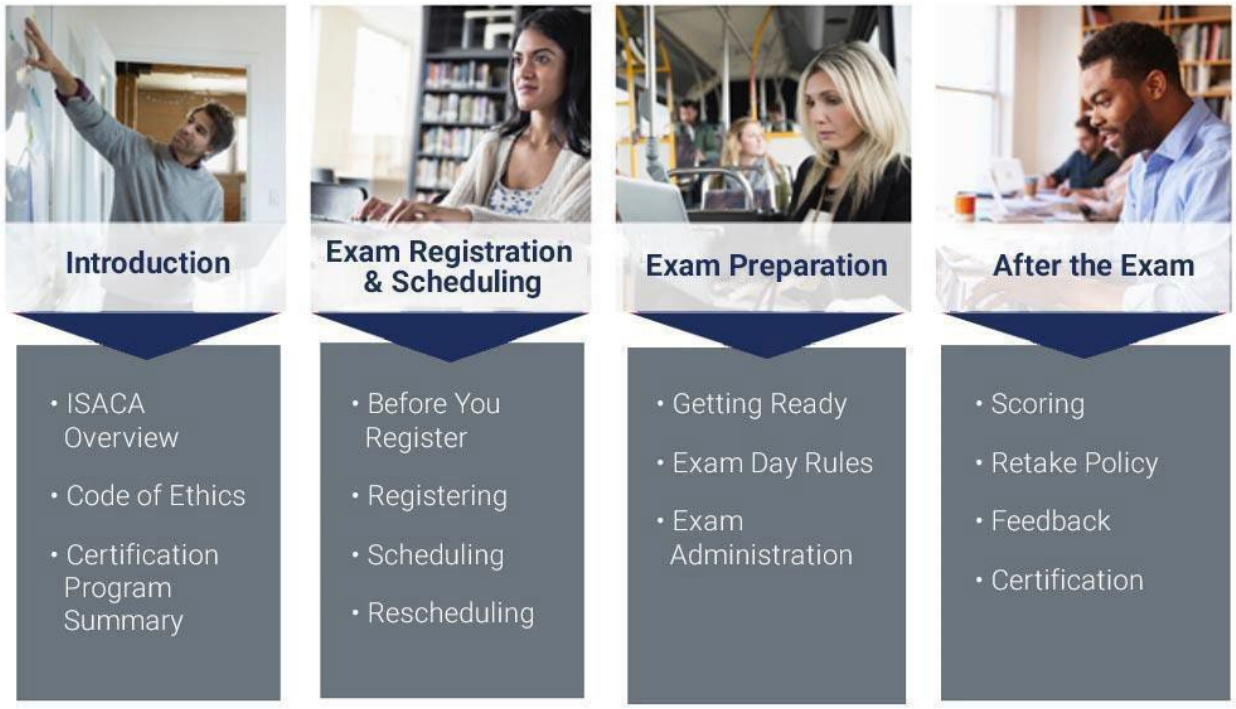
Table of Contents

Candidate Guide Overview

Review this guide thoroughly. It contains important details ISACA Exam Candidates need to know before administration of the exam, 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:

- 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 that helps individuals and enterprises achieve the positive potential of technology.

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

ISACA leverages the expertise of its more than 185,000+ members who work in digital trust fields such as information security, governance, assurance, risk, privacy, and quality, as well as its enterprise performance subsidiary, CMMI® Institute, to help advance innovation through technology.

ISACA has a presence in 190 countries, including more than 230 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 preparation 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 career progression and innovation in the workplace.

COBIT 2019®

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

Certificate Programs

A full list of ISACA's certificate programs can be found at: https://www.isaca.org/credentialing.

Certification Programs

Validate your experience and knowledge in IT audit, security, and control. Boost your career and salary potential.

The first advanced audit-specific AI certification for CISA, CPA, and CIA holders.

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

The first AI-centric security management certification for CISM and CISSP holders.

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

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

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

Empowers cybersecurity professionals to prove their hands-on abilities to employers.

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 table 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 and control, assurance, and information security professionals	Designed for those in 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 life cycle 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 risk management and compliance, privacy engineering, and/or data life cycle 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	**Domain 1** – Governance (26%) **Domain 2** – Risk Assessment (22%) **Domain 3** – Risk Response and Reporting (32%)	**Domain 1** – Information Security Governance (17%) **Domain 2** – Information Security Risk Management (20%) **Domain 3** – Information Security Program (33%)	**Domain 1** – Governance of Enterprise IT (40%) **Domain 2** – IT Resources (15%) **Domain 3** – Benefits Realization (26%)	**Domain 1** – Privacy Governance (20%) **Domain 2** – Privacy Risk Management & Compliance (18%) **Domain 3** – Data Lifecycle Management (23%) **Domain 4** – Privacy Engineering (39%)

	(12%) **Domain 4** – Information System Operation and Business Resilience (26%) **Domain 5** – Protection of Information Assets (26%)	**Domain 4** – Technology and Security (20%)	**Domain 4** – Incident Management (30%)	**Domain 4** – Risk Optimization(19 %)	
Exam Languages	English Spanish Chinese-Simplified French German Korean Japanese	English Spanish Japanese	English Spanish Chinese-Simplified Japanese French German	English Chinese-Simplified	English
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 nonrefundable and nontransferable.

Resources

Below are some useful links and resources to help 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, with 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. This means that from the date you register, you have 12 months (365 days) to take the exam. It is important to note that the exam registration fee must be paid in full before you 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 appear on your dashboard 90 days prior to the expiration of your eligibility. If an exam has been scheduled, it must be canceled 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 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. Candidates will also accept the conditions set forth in this Candidate Guide, including those covering exam administration, certification rules, and the release of test results.

Candidates cannot schedule a testing appointment until exam registration fees are paid in full. Exam fees are **nonrefundable** and **nontransferable.**

Registration Acknowledgment

Candidates will receive a **Notification to Schedule** email within one (1) business day following registration and payment. This email provides information on scheduling your exam appointment.

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: This form must be completed by you and your health care professional.**
4.	Submit the 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 four (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:

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. To update your name: 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	To change your preferred 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 must also reschedule the testing appointment.** See Rescheduling an Exam for details.
Exam Type	To request a change to the 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 nonrefundable and nontransferable.

You will forfeit your fees if you do not schedule and take the exam during your 12-month eligibility period. No eligibility extensions are allowed without the purchase of an exam eligibility extension.

Exam Scheduling

There are five key steps to schedule an exam appointment:

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

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

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 the 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 any time during the eligibility period, without penalty, a minimum of 48 hours prior to the 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 outlined in the Scheduling Guide.

Emergency Closing

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

Section III: Exam Preparation

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 the 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. A question may require you to choose the answer based on a qualifier, such as MOST likely or BEST.
- 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 before 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. Candidates have 4 hours to complete the CISA/CRISC/CISM/CGEIT exams and 3.5 hours to complete the CDPSE exam.

Exams at an In-Person Exam Center

If your exam is scheduled at an exam center, prepare before the day of the exam by:

- Locating the test center address and confirming the start time
- Mapping out your route to the testing center
- Planning to arrive at least 30 minutes prior to the exam start time
- Planning 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 a device, complete the compatibility check prior to exam day. If you are using a company device to take the exam, you may need your IT department's assistance or approval to download the secure browser.

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. The first and last name on the ID must match the name used to register for the exam, or you may not be permitted entry.
- Candidate's signature (driver's licenses issued in Japan without a signature are accepted)
- Candidate's photograph

All information must be demonstrated by a single form of ID (and cannot be a copy or handwritten). **Digital IDs are not accepted**. 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 ID

Acceptable forms of ID include:

- Driver's license
- State ID card (nondriver's license)
- Passport
- Passport card
- Green card
- Alien registration
- Permanent resident card
- National ID card

The testing center reserves the right to ask for additional forms of ID 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 will forfeit your exam fees. To take the exam in the future, you will be required to register and pay the exam fee again.

3.2 Exam Day Rules

The exam rules are guidelines regarding 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. Per these terms, ISACA has the right to nullify exam scores if any unacceptable behaviors are identified.

Prohibited Items

During the exam, the candidate's workspace must be completely clear of all other items and materials. You will be required to face toward the screen for the duration of the exam so the proctors can properly monitor the exam session.

Candidates are prohibited from having the following items with them throughout the duration of the exam:

- Reference materials, study materials, paper, notes, notepads, language dictionaries, or other aids
- Calculators
- Multiple monitors
- Any type of communication, surveillance, or electronic/recording devices, including but not limited to:
  - Mobile phones
  - 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 candidates are seen with any such communication, surveillance, or electronic/recording devices during administration of the exam, 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

Candidates should plan to store their 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, the following activities are prohibited:

- Creating a disturbance
- Giving or receiving assistance using notes, papers, or other aids; use of unauthorized study materials
- Talking, reading the questions out loud, or moving your lips while reading silently
- Copying, photographing, recording, memorizing, or otherwise attempting to retain or re-create any exam content or assisting anyone in retaining, recreating, or reconstructing exam content for any purpose
- Attempting to take the exam for someone else or having someone else take the exam for you
- Possession of a communication, surveillance, or electronic/recording device, including but not

limited to mobile devices, tablets, smart glasses, smart watches, etc.

- 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 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 from your proctor. During an approved break, the exam will be paused, but the timer will not stop.
- 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 the exam registration fee. To do this:

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

To contact PSI:

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

Examples of personal hardship include:

- Personal illness
  - Documentation such as a doctor's note, proof of an emergency room admittance, etc., is required:
    - Must be signed by a licensed doctor and include the date of the medical visit
    - Must include contact information for the licensed doctor
    - Does not need details about the illness or emergency
    - Should include indication from the doctor that the candidate should not take the exam due to the illness or emergency
- Death of an immediate family member, including a spouse, child/dependent, parent, grandparent, or sibling
  - Documentation must include the date of death, the deceased's name, and the candidate's relationship to the deceased
- Traffic accident
  - Documentation can include a police report or receipt from a mechanic or towing company, which includes the date and contact information

If a personal hardship request is denied, candidates are required to register and pay the full registration fee again.

Leaving the Testing Area

Candidates must gain authorization from the test proctor to leave the testing center. In the case of remotely proctored exams, they must gain authorization to leave the designated testing area. Leaving the testing center or area without authorization may result in your exam being terminated.

Two breaks are permitted with permission from your proctor. The exam will be paused, but the timer will not stop during an approved break.

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 a candidate violates the Terms of Use or exam day rules or engages in any kind of misconduct, they will be subject to the following:

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

3.3 Exam Administration

The exam can be administered at a PSI testing center or remotely 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.

3.4 Online Remote Proctoring

As mentioned, 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.

Candidates can communicate with remote proctors in English using a live chat tool during the exam. Other languages are not available for communicating with remote proctors.

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

Exam Rules for Online Proctoring

The exam is online, closed book, and remotely proctored. The proctor will stop the exam if any of the exam rules are not followed. Any form of cheating will not be tolerated and will result in a voided exam without a refund.

More specifically, the following scenarios are NOT allowed during testing:

- Having someone else in the room during the exam, such as other people standing in, or walking through, the testing area
- Taking breaks, including stepping away without the proctor's permission
- Using a camera, recording device, or any other electronic device(s), including smart devices such as watches and glasses
- Taking screenshots of the computer screen and/or exam items
- Having reference materials present including papers, books, or notes in the workspace
- Using other programs or applications on your system, which includes viewing documents, browsing, remote access, or email access
- Reading exam questions out loud, talking to someone else in the room, or talking to yourself
- Copying or writing down exam content
- Covering the camera or moving away from the camera's view (please note that proctors will warn you if you make the slightest move out of camera view)
- Eating, drinking, or chewing gum
- Looking away from the computer screen

Note: Failure to comply with any of the above will result in your exam being voided and forfeiture of your exam fees. If you have any questions regarding these requirements, please contact the ISACA Customer Experience Center by visiting https://support.isaca.org.

ISACA will require a mirror check for each exam following a 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 you use a mobile phone, it will need to be placed out of reach of the room designated for testing after the mirror check is complete.

Section IV: After the Exam

This section covers exam scoring and applying for certification.

4.1 Exam Scoring

Receiving Your Score

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

- The email notification will be sent to the email address listed on your profile.
- Online results will be available on the MyISACA > Certifications & CPE Management page.
- Exam scores will not be provided by telephone or fax.
- Question-level results are not 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 pretest items. Pretest items are not used to calculate exam scores. 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.
- Candidates 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-specific percentages indicate the portion of the exam that reflects that domain content and are not used to calculate exam scores.
- A candidate who receives a passing score can apply for certification if all other requirements are met (see How to Become Certified for more details).

Requests for Rescoring

While ISACA is 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.

Candidates must submit a rescore request in writing through the ISACA 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.

Individuals have four (4) attempts within a rolling 12-month period to pass the exam. Those that do not pass on their first attempt are allowed to retake the exam a total of three (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): Candidates must wait 30 days from the date of the first attempt.
- Retake 2 (attempt 3): Candidates must wait 90 days after the date of the second attempt.
- Retake 3 (attempt 4): Candidates must wait 90 days after the date of the third attempt.

Individuals who pass the exam are restricted from taking the same exam within the application time period of five (5) years.

Certification holders are restricted from taking the same certification exam while they are certified.

4.3 Post-Exam Feedback

Candidates 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

Candidates may provide comments and concerns about the exam 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. To submit comments:

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 US$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 five (5) years from passing the exam to apply for certification. Additional resources include:

- Pass the examination: CISA | CISM | CGEIT | CRISC | CDPSE
- Pay the US$50 application processing fee: CISA | CISM | CGEIT | CRISC | CDPSE
- Submit the application for certification: CISA | CISM | CGEIT | CRISC | CDPSE
- Adhere to ISACA's Code of Professional Ethics, Terms of Use, and Privacy Notice
- Adhere to the Continuing Professional Education (CPE) Policy: CISA | CISM | CGEIT | CRISC |CDPSE
- Comply 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 needed 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 earning potential
- Counts in the hiring process
- Enhances 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 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. The accreditation details are as follows:

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."

Appendices

Appendix A: CISA

CISA Examination Content Outline

(Effective August 2024)

1	**Information System Auditing Process**	**18%**
1A	Planning	
1A1	IS Audit Standards, Guidelines, Functions, and Codes of Ethics	
1A2	Types of Audits, Assessments, and Reviews	
1A3	Risk-Based Audit Planning	
1A4	Types of Controls and Considerations	
1B	Execution	
1B1	Audit Project Management	
1B2	Audit Testing and Sampling Methodology	
1B3	Audit Evidence Collection Techniques	
1B4	Audit Data Analytics (including audit algorithms)	
1B5	Reporting and Communication Techniques	
1B6	Quality Assurance and Improvement of Audit Process	
2	**Governance and Management of IT**	**18%**
2A	IT Governance	
2A1	Laws, Regulations, and Industry Standards	
2A2	Organizational Structure, IT Governance, and IT Strategy	
2A3	IT Policies, Standards, Procedures and Practices	
2A4	Enterprise Architecture (EA) and Considerations	
2A5	Enterprise Risk Management (ERM)	
2A6	Privacy Program and Principles	
2A7	Data Governance and Classification	
2B	IT Management	
2B1	IT Resource Management	
2B2	IT Vendor Management	
2B3	IT Performance Monitoring and Reporting	
2B4	Quality Assurance and Quality Management of IT	
3	**Information Systems Acquisition, Development, and Implementation**	**12%**
3A	Information Systems Acquisition and Development	
3A1	Project Governance and Management	
3A2	Business Case and Feasibility Analysis	
3A3	System Development Methodologies	
3A4	Control Identification and Design	
3B	Information Systems Implementation	
3B1	System Readiness and Implementation Testing	
3B2	Implementation Configuration and Release Management	
3B3	System Migration, Infrastructure Deployment, and Data Conversion	
3B4	Post-Implementation Review	

4	**Information Systems Operations and Business Resilience**	**26%**
4A	Information Systems Operations	
4A1	IT Components	
4A2	IT Asset Management	
4A3	Job Scheduling and Production Process Automation	
4A4	System Interfaces	
4A5	Shadow IT and End-User Computing (EUC)	
4A6	Systems Availability and Capacity Management	
4A7	Problem and Incident Management	
4A8	IT Change, Configuration, and Patch Management	
4A9	Operational Log Management	
4A10	IT Service Level Management	
4A11	Database Management	
4B	Business Resilience	
4B1	Business Impact Analysis (BIA)	
4B2	System and Operational Resilience	
4B3	Data Backup, Storage, and Restoration	
4B4	Business Continuity Plan (BCP)	
4B5	Disaster Recovery Plans (DRP)	
5	**Protection of Information Assets**	**26%**
5A	Information Asset Security and Control	
5A1	Information Asset Security Policies, Frameworks, Standards, and Guidelines	
5A2	Physical and Environmental Controls	
5A3	Identity and Access Management	
5A4	Network and End-Point Security	
5A5	Data Loss Prevention (DLP)	
5A6	Data Encryption	
5A7	Public Key Infrastructure (PKI)	
5A8	Cloud and Virtualized Environments	
5A9	Mobile, Wireless, and Internet-of-Things (IoT) Devices	
5B	Security Event Management	
5B1	Security Awareness Training and Programs	
5B2	Information System Attack Methods and Techniques	
5B3	Security Testing Tools and Techniques	
5B4	Security Monitoring Logs, Tools, and Techniques	
5B5	Security Incident Response Management	
5B6	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

CRISC Examination Content Outline
(Effective 2025)

1	**Governance**	**26%**
1A	Organizational Governance	
1A1	Strategy, Goals, and Objectives	
1A2	Organizational Structure, Roles, and Responsibilities	
1A3	Organizational Culture and Ethics	
1A4	Policies and Standards	
1A5	Business Processes and Resilience (e.g., DRP, BCP)	
1A6	Organizational Asset Management	
1B	Risk Governance	
1B1	Enterprise Risk Management (ERM)	
1B2	Lines of Defense	
1B3	Risk Profile	
1B4	Risk Appetite and Risk Tolerance	
1B5	Risk Frameworks, Legal, Regulatory, and Contractual Requirements	
2	**Risk Assessment**	**22%**
2A	Risk Identification	
2A1	Risk Events	
2A2	Threat Modeling and Threat Landscape	
2A3	Vulnerability Management	
2A4	Risk Scenario Development and Evaluation	
2B	Risk Analysis	
2B1	Risk Assessment Concepts and Standards	
2B2	Business Impact Analysis (BIA)	
2B3	Risk Register	
2B4	Risk Analysis Methodologies	
2B5	Inherent and Residual Risk	
3	**Risk Response and Reporting**	**32%**
3A	Risk Response	
3A1	Risk Response Options	
3A2	Risk and Control Ownership	
3A3	Vendor/Supply Chain Risk Management	
3A4	Issues, Findings, Exceptions and Exemptions Management	
3B	Control Design and Implementation	
3B1	Control Frameworks, Types, and Standards	
3B2	Control Design, Selection, Implementation, and Analysis	
3B3	Control Testing Methodologies	
3C	Risk Monitoring and Reporting	
3C1	Risk Action Plans	
3C2	Data Collection, Aggregation, Analysis, and Validation	

3C3	Risk and Control Metrics (e.g., KRIs, KCIs, KPIs)	
3C4	Risk and Control Monitoring Techniques	
3C5	Risk and Control Reporting Techniques (e.g., heatmap, scorecards, dashboards)	
3C6	Monitoring and Reporting of Emerging Risks	
4	**Technology and Security**	**20%**
4A	Technology Principles	
4A1	Technology Roadmaps and Enterprise Architecture (EA)	
4A2	Operations Management (e.g., change management, assets, DevOps, problems, incidents)	
4A3	System Development Life Cycle (SDLC)	
4A4	Data Lifecycle Management	
4A5	Portfolio and Project Management (e.g. Agile)	
4A6	Technology Resilience and Disaster Response/Recovery	
4A7	Emerging Technologies	
4B	Information Security Principles	
4B1	Security Concepts, Frameworks, and Standards	
4B2	Security/Risk Awareness and Training	
4B3	Data Privacy and Data Protection Principles	

SupportingTasks

1. Collect, review, and evaluate existing information regarding the organization’s business and information system environments.
2. Identify potential or realized impacts of information system risk to the organization’s business objectives and operations.
3. Identify threats and vulnerabilities to the organization’s people, processes, and technologies.
4. Evaluate threats, vulnerabilities, and risk to create information system risk scenarios.
5. Establish accountability by assigning and validating appropriate levels of risk and control ownership.
6. Maintain or establish the information system risk register and incorporate it into the enterprise-wide risk profile.
7. Assist key stakeholders in the selection of risk appetite and tolerance thresholds and the impact on business objectives.
8. Promote a risk-aware culture by contributing to the development and implementation of security/risk awareness and training.
9. Conduct a risk assessment by analyzing information system risk scenarios and events to generate a risk score/rating.
10. Identify the current state of existing controls and evaluate their effectiveness for information system risk treatment.
11. Determine if risk exceeds appetite and tolerance thresholds to recommend treatment options and rectify concerns.
12. Review the results of risk and/or control analysis to assess any gaps between current and desired states of the risk environment.

13. Collaborate with risk owners on the development of risk treatment plans.
14. Collaborate with control owners on the selection, design, implementation, and maintenance of controls.
15. Validate that risk responses have been executed according to risk action plans.
16. Define, implement, and refine key risk indicators (KRIs).
17. Collaborate with control owners on the identification and refinement of key performance indicators (KPIs) and key control indicators (KCIs).
18. Monitor and analyze key risk indicators (KRIs), key performance indicators (KPIs), and key control indicators (KCIs).
19. Review the results of control assessments to determine the adequacy, effectiveness, and maturity of the control environment.
20. Conduct aggregation, analysis, and validation of risk and control data.
21. Report relevant risk and control information to applicable stakeholders to facilitate risk-based decision-making.
22. Evaluate emerging technologies and changes to the environment for threats, vulnerabilities, and opportunities.
23. Evaluate alignment of business practices with risk management frameworks, standards, and regulations.
24. Facilitate tabletop exercises to verify and identify gaps in risk scenarios, capabilities, and responses.

Appendix C: CISM

CISM Examination Content Outline
(Effective 2022)

1	Information Security Governance 17%	
1A	Enterprise Governance	
1A1	Organizational Culture	
1A2	Legal, Regulatory, and Contractual Requirements	
1A3	Organizational Structures, Roles, and Responsibilities	
1B	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%
2A	Information Security Risk Assessment	
2A1	Emerging Risk and Threat Landscape	
2A2	Vulnerability and Control Deficiency Analysis	
2A3	Risk Assessment and Analysis	
2B	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%
3A	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	
3B	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%
4A	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

4B 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

CGEIT Examination Content Outline

(Effective 2020)

1	**Governance of Enterprise IT**	**40%**
1A	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	
1B	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	
1C	Information Governance	
1C1	Information Architecture	
1C2	Information Asset Lifecycle	
1C3	Information Ownership and Stewardship	
1C4	Information Classification and Handling	
2	**IT Resources**	**15%**
2A	IT Resource Planning	
2A1	Sourcing Strategies	
2A2	Resource Capacity Planning	
2A3	Acquisition of Resources	
2B	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**	**26%**
3A	IT Performance and Oversight	
3A1	Performance Management	
3A2	Change Management	
3A3	Governance Monitoring	
3A4	Governance Reporting	
3A5	Quality Assurance	
3A6	Process Development and Improvement	
3B	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**	**19%**

4A	Risk Strategy
4A1	Risk Frameworks and Standards
4A2	Enterprise Risk Management
4A3	Risk Appetite and Risk Tolerance
4B	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

CDPSE Examination Content Outline
(Effective 2025)

1	**Privacy Governance**	**20%**
1A	Privacy Governance	
1A1	Personal Information	
1A2	Privacy Principles (e.g., Privacy by Design, Consent, Transparency)	
1A3	Privacy Laws and Regulations	
1A4	Privacy Documentation (e.g., Policies, Guidelines)	
1B	Privacy Operations	
1B1	Organizational Culture, Structure, and Responsibilities	
1B2	Vendor and Supply Chain Management	
1B3	Incident Management	
1B4	Data Subject Rights, Requests, and Notification	
2	**Privacy Risk Management and Compliance**	**18%**
2A	Risk Management	
2A1	Risk Management Process and Policies	
2A2	Privacy-Focused Assessment (e.g., Privacy Impact Assessment (PIA))	
2A3	Privacy Training and Awareness	
2A4	Threats and Vulnerabilities	
2A5	Risk Response	
2B	Compliance	
2B1	Privacy Frameworks	
2B2	Evidence and Artifacts	
2B3	Program Monitoring and Metrics	
3	**Data Life Cycle Management**	**23%**
3A	Data Collection and Processing	
3A1	Data Inventory, Dataflow Diagram, and Classification	
3A2	Data Quality (e.g. Accuracy)	
3A3	Data Use Limitation	
3A4	Data Analytics (e.g., Aggregation, AI, Data Warehouse)	
3B	Data Persistence and Destruction	
3B1	Data Minimization	
3B2	Data Disclosure and Transfer	
3B3	Data Storage, Retention, and Archiving	
3B4	Data Destruction	
4	**Privacy Engineering**	**39%**
4A	Technology Stacks	
4A1	Infrastructure and Platform Technology (e.g., legacy, cloud computing)	
4A2	Devices and Endpoints	
4A3	Connectivity	

4A4	Secure Development Life Cycle
4A5	APIs and Cloud-Native Services
4B	Privacy Related Security Controls
4B1	Asset Management
4B2	Identity and Access Management
4B3	Patch Management and Hardening
4B4	Communication and Transport Protocols
4B5	Encryption and Hashing
4B6	Monitoring and Logging
4C	Privacy Controls
4C1	Consent Tagging
4C2	Tracking Technologies (e.g., cookie management)
4C3	Anonymization and Pseudonymization
4C4	Privacy Enhancing Technologies (PETs)
4C5	AI/Machine Learning (ML) Considerations

Supporting Tasks

1. Identify internal and external requirements to develop and maintain the organization's privacy programs.
2. Review organizational programs to align with privacy related legal and regulatory requirements, industry best practices (e.g., privacy by design), and data subject's expectations.
3. Advise on data life cycle policies and practices to ensure privacy considerations for data governance.
4. Design and evaluate the implementation of technical and operational controls for data classifications and data life cycle requirements.
5. Perform privacy impact assessments (PIAs) and other privacy-focused assessments.
6. Contribute to the integration of privacy principles (e.g., privacy by design) in the development of procedures and operational manuals for organizational needs.
7. Collaborate with stakeholders to promote privacy principles (e.g., privacy by design) are followed during the design, development, and implementation of systems, applications, and infrastructure.
8. Identify and assess privacy related threats and vulnerabilities.
9. Contribute to the evaluation of contracts, service level agreements (SLAs), and privacy practices of vendors and other parties and subsequently monitor for compliance.
10. Participate in the incident management process to address privacy impacts and support remediation.
11. Collaborate with relevant stakeholders to address privacy compliance and risk response.
12. Contribute to the evaluation of information architecture to support privacy by design principles and data considerations.
13. Evaluate changes in regulatory landscape, emerging threats to privacy, and privacy enhancing technologies (PETs).
14. Design, implement, and monitor processes and procedures to keep personal information inventory and dataflow records current and accurate.
15. Advise on data classification for personal information to enable risk assessment and implementation of controls.
16. Develop and monitor metrics to report on privacy program performance to relevant stakeholders.
17. Advocate for advancing privacy posture and maturity as it aligns to the organizational objectives.
18. Contribute to the development of educational content and conduct privacy training to promote a privacy aware culture.
19. Promote accountability, fairness, and transparency throughout the data life cycle.

