



# GRCP Candidate Handbook



# Table of Contents

About OCEG	3
About GRC Certify	4
Purpose & Promise	4
Accreditation	4
GRC Certify Standards	4
Best Practices	5
Unified Certification Program Structure	7
Certification Development Process	7
General Eligibility	7
Preparing for an Exam	8
Scheduling an Exam	8
Taking an Exam	9
Special Accommodations	10
Unified Certification Exam, Recertification & Continuing Professional Education (CPE) Structure	11
Credential Certificates & Badges	11
Credential Verification	12
Continuing Education	12
Double Counting	12
Electronic Tracking	13
Recertification	13
Auditing	13
Complaints & Appeals	13
GRC Professional (GRCP) Certification	15
GRCP Exam Blueprint	15
GRCP Exam Sample Questions	16

## About OCEG

OCEG is a global nonprofit think tank that created Principled Performance and GRC in 2003. Every year thousands of GRC Professionals are trained and prepared to pass exams administered by GRC Certify.

At OCEG, GRC Professionals gain a versatile, interdisciplinary skillset to solve some of the most vexing problems caused by unprincipled misconduct, mistakes, and miscalculations – problems that result in over \$1 Trillion USD of damage every year.

An important GRC insight is that these big problems require an interdisciplinary approach.



In this sense, GRC is like an “umbrella” over several Critical Disciplines. GRC Professionals are skilled at the breadth, depth, and integration of these disciplines. Thus, GRC Professionals typically serve in departments such as: the Board of Directors, Executive Team, Strategy, Performance, Risk, Compliance & Ethics Management, IT Security, Business Continuity, Internal Controls, Quality Management, Human Resources, Audit & Assurance. Despite the diverse roles, departments, and job titles, GRC Professionals are bonded by a common Code for GRC Professionals (also known as “The Protector Code”).

OCEG provides a streamlined, end-to-end experience for GRC Professionals to prepare for and pass certification exams accredited by GRC Certify.

# About GRC Certify

GRG Certify is a global nonprofit organization founded in 2010 to help GRC Professionals demonstrate their skills through certification exams. GRG Certify governs the certification process for organizations that offer certifications in one or more of the Critical Disciplines.

## Purpose & Promise

As an organization, GRG Certify aims to help GRC Professionals become versatile, collaborative, and accountable executives by setting and testing high standards of knowledge and skill. GRG Certify continuously improves its approach to be ever more accessible, applicable, and valuable so that every individual has the opportunity to excel.

## Accreditation

GRG Certify follows best practices for professional certification and certificate programs. Several organizations publish these standards, and GRG Certify uses a “best of breed” approach to deliver a modern experience for professional certification.

GRG Certify is consistent with standards specific to Job Task Analysis (JTA), Subject Matter Expert (SME) Involvement, required prerequisites, test blueprint creation, item development, test design, setting cut-score, exam updates, recertification, and certification revocation.

GRG Certify ensures the security and integrity of all assessments, as well as exam administration using leading-edge security.

## GRG Certify Standards

GRG Certify requires that all accredited organizations meet 10 Standards:

- Standard 1: Content Alignment
  1. Define essential skills with job task analysis (JTA).

2. Systematically develop the body of knowledge.
- Standard 2: Quality Testing
  1. Use psychometric standards for examinations.
  2. Create fair, reliable, and valid exam items.
- Standard 3: Impartial Oversight
  1. Objectively and competently govern the program.
  2. Avoid conflicts of interest.
- Standard 4: Candidate Requirements
  1. Set clear eligibility criteria for candidates.
  2. Define recertification and continuing education rules.
- Standard 5: Operational Excellence
  1. Administer secure and efficient exam processes.
  2. Protect candidate privacy and confidentiality.
- Standard 6: Continuous Improvement
  1. Conduct quality checks.
  2. Periodically review and update content.
- Standard 7: Stakeholder Engagement
  1. Involve candidates, experts, and employers.
  2. Encourage feedback and transparency.
- Standard 8: Documentation Standards
  1. Provide necessary documents for accreditation.
  2. Prepare for third-party audits and reviews.
- Standard 9: Legal and Ethical Compliance
  1. Follow legal and ethical standards.
  2. Protect intellectual property and data.

- Standard 10: Clear Communication
  1. Communicate openly with stakeholders.
  2. Share policies, procedures, and program changes.

GRC Certify aims to help GRC Professionals become versatile professionals who embody The Protector Code by setting and testing for high standards of knowledge and skill.

## Best Practices

GRC Certify aims to ensure that its certifications strive to meet accreditation standards and best practices through entities, including:

- ICE (Institute of Credentialing Excellence),
- ANSI (American National Standards Institute), and
- NCCA (National Commission for Certifying Agencies).

### American National Standards Institute (ANSI)

GRC Certify is a member of the American National Standards Institute (ANSI). ANSI oversees standards and conformity assessment activities in the United States.

As the only accreditor of American National Standards Developers and approver of American National Standards (ANS), ANSI gets members actively involved in the ANSI process. In support of the public-private partnership at the core of the U.S. system's strength, ANSI's standards coordination activities provide a neutral forum for all stakeholders to come together and identify consensus-based standardization solutions that meet national needs.

In the global arena, ANSI is the U.S. representative to the International Organization for Standardization (ISO) and to the International Electrotechnical Commission (IEC), through the U.S. National Committee (USNC), among other international and regional standardization organizations. Through ANSI, U.S. stakeholders have immediate access to the ISO and IEC standards development processes. And, the ability to administer a delegated international Secretariat or U.S. Technical Advisory Group (TAG) to an ISO or IEC committee offers members the chance work

with a wide array of stakeholders and leaders from industry, government, private companies, educational institutions, consumer groups, and other organizations on creative solutions to emerging issues and obstacles that affect your industry or area of interest. (Ref: <https://www.ansi.org/membership/member-benefits>)

## Institute of Credentialing Excellence (ICE)

GRC Certify is a member of the Institute for Credentialing Excellence (ICE). This professional membership association provides education, networking, and other resources for organizations and individuals who work in and serve the credentialing industry. ICE is a leading developer of standards for both certification and certificate programs, and it is both a provider of and a clearing house for information on trends in certification, test development and delivery, assessment-based certificate programs, and other information relevant to the credentialing community. (Ref: <https://www.credentialingexcellence.org/About>)

## National Commission for Certifying Agencies (NCCA)

GRC Certify considers the National Commission for Certifying Agencies (NCCA) standards, consistent with the Standards for Educational and Psychological Testing (AERA, APA, & NCME, 1999), and is applicable to all professions and industries. (Ref: <https://www.credentialingexcellence.org/Accreditation/Earn-Accreditation/NCCA>)

# Unified Certification Program Structure

Each certification governed by GRC Certify follows a unified program structure. Each certification has a specific section that highlights the details that certification's exam blueprint, sample questions, and any deviations from the unified structure.

## Certification Development Process

GRC Certify creates each certification using a phased development process. GRC Certify formulates this process based on accreditation standards and best practices, including developing and managing the exam to support reliability, validity, and security.

Each certification goes through development stages, including:

- Job Task Analysis (JTA).
- Essential Body of Knowledge (BoK) Development.
- Exam Blueprint.
- Item Development and Test Design.
- Pilot.
- Beta Copy & Standard-Setting.
- Production.
- Maintenance.

✉ For any questions related to the certification development process for any GRC Certify exam, contact [support@grccertify.org](mailto:support@grccertify.org)

## General Eligibility

GRC Certify certifications are open and accessible to all professionals. We accept candidates from diverse cultural, educational, and professional backgrounds. Candidates for GRC Certify certifications include anyone who adheres to [The Protector Code](#).

\* GRC Certify works with training partners and membership associations. These organizations often bundle these costs into discounted packages. For example, OCEG offers an [All Access Pass and various team bundles](#) that include unlimited exams and retakes as part of a discounted membership.

## Preparing for an Exam

Each GRC Certify certification outlines the Body of Knowledge (BoK) in the candidate handbook. The BoK materials are generally available and often open source. The exam assesses knowledge used by a “typical” professional in a “typical” job associated with the BoK. Within each handbook, sample questions for each exam are also included. Refer to the specific exam’s handbook to see the associated BoK materials and sample questions.

GRC Certify exams typically do not require previous job experience, though previous experience does help candidates to pass the exam.

Authorized training partners offer in-person and online courses if candidates are interested in more directed exam preparation.

\* A list of authorized training partners is available on the [OCEG website](#).

## Scheduling an Exam

GRC Certify exams are online, available anytime, and taken anywhere, and do not require proctoring.

Our approach to certification is one that believes in the following

1. **Online Security Measures:** Our examination platform is fortified with cutting-edge online security measures, including multi-factor authentication, encrypted connections, and secure browser technology. These protocols prevent unauthorized access, safeguarding the integrity of the exam process.
2. **Data Analytics for Anomaly Detection:** Leveraging sophisticated data analytics, we continually analyze exam results for any anomalies or irregular patterns, enabling us to identify and address any potential misconduct swiftly and effectively. This approach allows us to maintain exam integrity in a virtual environment.
3. **User-Friendly Experience for Candidates:** Providing a user-friendly and flexible exam experience is paramount to us. Embracing a non-proctored model allows candidates to schedule exams at their convenience, reducing any unnecessary stress associated with traditional in-person proctoring.
4. **Accessibility and Inclusivity:** Our non-proctored exam model ensures that candidates, regardless of location or physical ability, can participate in the assessment process. This inclusivity aligns with our commitment to fostering a diverse and talented community of professionals.
5. **Cost-Effectiveness and Efficiency:** By adopting a modern approach, we can allocate resources more efficiently, ultimately reducing administrative burdens and costs. This optimization allows us to invest in further enhancing the quality and scope of our certification programs.

## Taking an Exam

Before taking an exam, candidates should ensure that they understand the body of knowledge aligned with the specific certification.

After submitting all answers, the candidate's score is immediately available. If candidates pass, they receive their passing score and an online certificate.

If candidates fail, the candidate must follow the certification exam retesting policies and procedures.

GRC Certify designs exam questions rigorously and aligns question content with current GRC-industry practices, knowledge, and skills. GRC Certify tests candidate knowledge and skill in real-world situations. This means that candidates may use notes and resources during the exam – just like the real-world.

## Retaking an Exam (Retesting)

If a candidate does not achieve a passing score on the first attempt, the candidate should wait 48 hours before retaking the exam. GRC Certify recommends that candidates use this time to focus on refreshing their understanding of relevant content.

If a candidate does not achieve a passing score on the second attempt, the candidate should wait at least 14-days before retaking the exam. This waiting period follows current industry norms and best practices for retesting. This timeframe allows candidates to prepare further and assess their knowledge and understanding.

A candidate is not eligible to take the exam more than six (6) times in any 12 months. This specification follows current industry norms and best practices for retesting. The 12-month period begins on the date of their first certification exam attempt. The candidate is eligible to retake the exam 12 months from the date of their first attempt.

## Special Accommodations

GRC Certify complies with the Americans with Disabilities Act (42 U.S.C §12101 et seq.) and Title VII of the Civil Rights Act, as amended (42 U.S.C. §2000e et seq.) to assist individuals who need reasonable accommodations.

Reasonable accommodations provide individuals with disabilities a fair and equal opportunity to demonstrate their knowledge and skill. Reasonable accommodations are based on the individual's request, disability, documentation submitted, and appropriateness of the proposal – but shall not include actions that fundamentally alter the purpose or nature of the exam.

GRC Certify provides accommodations within a reasonable timeframe, except where it may fundamentally alter the exam, influence the exam results, or result in an undue burden.

- ✉ Accommodation requests should be submitted before accessing the exam by contacting [support@grccertify.org](mailto:support@grccertify.org).

# **Unified Certification Exam, Recertification & Continuing Professional Education (CPE) Structure**

Each GRC Certify exam shares the following structure unless a certification explicitly extends or overrides these items, which will be captured in the specific certification's section of each handbook.

Allotted Exam Time	2 hours (120 minutes)
Number of Exam Questions	100 (from a bank of at least 200 questions)
<b>Passing Score/Cutscore</b> <i>**Angoff method may adjust cut-score for certain exams</i>	70 correctly answered questions (out of 100)
Price	\$499 per exam, Included in the "All Access Pass"
Retake Price	Included in the "All Access Pass"
Maintenance Rules	8 units of continuing professional education (CPE) per year
Recertification Cycle	Every 5 years

<b>Recertification Price</b>	Included in the “All Access Pass”
------------------------------	-----------------------------------

## Credential Certificates & Badges

Passing candidates may use a GRC Certify designation and any related designations on their transcripts, social media platforms, email signatures, or other platforms showcasing certifications.

A digital certificate and badge document a candidate’s designation, including any “letters” that may be used in professional signatures.

The digital certificate is a high-resolution file that may be printed and framed.

## Credential Verification

Certificates are issued digitally and recorded to a blockchain system of record. Each certificate has a unique URL that allows employers or other stakeholders to verify the credentials in real-time.

If the certificate is not in digital form but printed in hardcopy, it contains a QR code that can be used for verification. Stakeholders may use a QR reader on a smartphone to scan the QR code on the certificate to navigate to an online service that verifies the printed certificate.

In cases where stakeholders are not able to use online verification, GRC Certify provides guided support to verify credentials via [support@grccertify.org](mailto:support@grccertify.org)

✉ In cases where stakeholders are not able to use online verification, GRC Certify provides guided support to verify credentials via [support@grccertify.org](mailto:support@grccertify.org)

## Continuing Professional Education

Part of being a certified professional is staying up-to-date with current practices. Each certification requires eight units of continuing professional education (CPE) each year.

A continuing education unit represents approximately 60 minutes of instruction – though, in the modern context, watching courses at 1.25x or 1.5x speed sometimes means that this time duration does not equate to CPE units.

## Double Counting

GRC Certify recognizes that often, CPEs can address more than one topic at a time. As such, a single continuing education course may count toward multiple certifications.

### ILLUSTRATIVE EXAMPLE

A course on “Risk Assessment” is relevant for both GRC Professional (GRCP) and GRC Audit (GRCA) certification. Thus, one hour of continuing education counts for TWO units of continuing education. ONE unit for GRCP and ONE unit for GRCA.

## Electronic Tracking

GRC Certify requires that all CPE education providers implement an electronic tracking system, making it easier for professionals to get credit for CPEs without the burden of forms and manual tracking.

That said, individuals may add or make corrections to CPEs manually.

For all manual CPEs, it is important for candidates to request a certificate directly from CPE event sponsors. It is up to candidates to review and verify all CPE submissions manually sent to the tracking platform to seek continued renewal of a GRC Certify credential.

## Recertification

All GRC Certify Certifications require recertification every five (5) years based on industry standards and best practices.

## Auditing

GRC Certify conducts audits that include:

- Retesting (Retaking the exam) audits - GRC Certify ensures that a candidate has not taken the certification exam more than six (6) times in any 12 months. This specification follows current industry norms and best practices for retesting. The 12-month period begins on the date of their first exam attempt.
- Continuing Professional Education (CPE) audits - GRC Certify ensures that a candidate has submitted their required units of CEs based on the requirements for each certification. GRC Certify aims to work with CPE providers who automatically track and send information to GRC Certify. The individual tracks documentation and can manually correct any mistakes.

## Complaints & Appeals

Adverse decisions by GRC Certify may include but are not limited to:

1. Denial of candidate application;
2. Denial of certification;
3. Denial of continuing education;
4. Denial of certification renewal; and
5. Revocation of certification.

In the event of an adverse decision in the areas outlined above, GRC Certify shall advise the individuals involved in the decision and the procedure for appealing the adverse decision. The individual desiring to appeal GRC Certify's adverse decision (the "Grievant") must adhere to the following guidelines and associated timelines.

The request must be received within sixty (60) days after GRC Certify notices the adverse decision. The candidate is responsible for demonstrating clear and convincing evidence to grant an appeal. GRC Certify shall review the request and notify the applicant of its determination. To request a copy of the full Appeal Policy, please contact GRC Certify at support@grccertify.org

All administrative practices and procedures, including appeals, will be non-discriminatory based on age, race, creed, color, religion, lifestyle, national origin, gender, sexual orientation, veteran status, or disability.

# GRC Professional (GRCP) Certification

The GRCP certification follows the Unified Certification Program Structure. The following information is specific to the GRCP.

## GRCP Exam Blueprint

The GRCP certification exam is based on a blueprint that serves as a competency model for GRC professionals. This blueprint was developed through an extensive job analysis and research involving over 1,000 GRC professionals who analyzed over 200 skills to determine their significance in the field of GRC. In September 2023, an updated JTA was conducted and further validation of the exam blueprint was established.

The GRCP certification exam assesses your knowledge and ability to apply the GRC Capability Model. The exam content is weighted as follows:

### 30% GRC Key Concepts

- Understand key concepts associated with
  - Reliably Achieving Objectives
  - Reliably Addressing Uncertainty
  - Reliably Acting with Integrity
- Understand key concepts associated with the Lines of Accountability™ and Integrated Action & Control Model™
- Understand key concepts associated with measuring the GRC Capability

### Model 70% GRC Capability Model Details

- Understand components, elements, and practices
- Understand key actions and controls
- Understand design and implementation considerations
- Details are grouped by components (adds up to 70%)
  - Learn Component: 15%
  - Align Component: 20%
  - Perform Component: 25%

- Review Component: 10%

The exam ensures that you understand:

1. Principles, outcomes, and key terms. Prove that you can communicate across disciplines using a common and unambiguous vocabulary.
2. Core components, practices, and activities. Demonstrate understanding of the components and elements of the GRC Capability model.
3. Relationship of GRC to disciplines. Discuss how GRC incorporates the governance, management, and audit of strategy, performance, risk, and compliance.

## GRCP Exam Sample Questions

Whether you are engaging in self-study of the GRC Capability Model, using OCEG's on-demand certification prep course (GRC Fundamentals), or attending a deeper dive course presented by one of OCEG's training partners, you can use the following sample questions to see how the exam is structured. These samples are live questions in the test databank; and therefore, some of these questions may be on your exam if they are randomly selected.

1. What is the essence or the central meaning of GRC?
  - A. To provide guidelines for managing financial risks and ensuring fiscal responsibility
  - B. To create a roadmap for achieving operational excellence and maximizing efficiency
  - C. To provide a framework that helps organizations achieve Principled Performance by integrating the Critical Disciplines, including governance, risk management, and compliance
  - D. To establish a set of best practices for corporate governance and board-level decision-making
2. In the context of GRC, which is the best description of the role of assurance in an organization?
  - A. Allocating financial resources and evaluating their use to manage the

organization's budget better

- B. Providing the governing body with opinions on how well its objectives are being met based on expertise and experience
- C. Designing and maintaining the organization's information technology systems to be accurate and reliable so management can be assured of meeting established objectives
- D. Objectively and competently evaluating subject matter to provide justified conclusions and confidence

3. What is the difference between leading indicators and lagging indicators?

- A. Leading indicators provide information or clues about future events or conditions, while lagging indicators provide information about past events or conditions
- B. Leading indicators are only used by top management, while lagging indicators are used by all employees
- C. Leading indicators are financial metrics, while lagging indicators are non-financial metrics
- D. Leading indicators are subjective measures, while lagging indicators are objective measures

4. What is the role of key risk indicators (KRIs)?

- A. KRIs are used to evaluate the performance of the risk management and compliance departments
- B. KRIs are indicators that help govern, manage, and provide assurance about risk related to an objective
- C. KRIs are only relevant for governmental entities and have no role in commercial enterprises
- D. KRIs are subjective measures that are not based on any specific risk assessments or data so they only provide a high-level assessment of threats

5. What is the duality of compliance, and how does it relate to risk?

- A. The duality of compliance involves addressing both compliance with obligations and compliance-related risks. Compliance involves meeting mandatory and voluntary obligations, while compliance-related risks involve addressing the risk of negative outcomes associated with non-compliance.
  - B. The duality of compliance refers to the balance between financial gains and ethical considerations in business decisions.
  - C. The duality of compliance refers to the distinction between domestic and international regulations that an organization must follow.
  - D. The duality of compliance refers to the trade-off between investing in compliance measures and allocating resources to other business areas.
6. What are the four key elements that the LEARN component focuses on understanding?
- A. Policies, controls, communication, and education
  - B. Monitoring, assurance, improvement, and analysis
  - C. Stakeholders, external context, internal context, and culture
  - D. Direction, objectives, identification, and design
7. What practices are involved in analyzing and understanding an organization's ethical culture?
- A. Implementing a performance appraisal system to evaluate employee performance
  - B. Analyzing the climate and mindsets about how the workforce generally demonstrates integrity
  - C. Conducting a survey of employees every few years on their views about the organization's commitment to ethical conduct
  - D. Developing a strategic plan to achieve the organization's long-term goals for improving ethical culture
8. An organization should compare its culture and subcultures to:
- A. External benchmarks with industry peers

- B. Expert views on what an ethical business culture should be
  - C. Best practice examples
  - D. Internal baselines because culture is idiosyncratic and difficult to compare to others
9. TRUE or FALSE. Identification typically uses only quantitative methods to identify and classify opportunities, obstacles, and obligations.
10. How is effectiveness measured in the context of the REVIEW component?
- A. Through the design and operating effectiveness of the capabilities to monitor the capability, provide assurance, and learn from prior mistakes and improve
  - B. Through the number of new products launched
  - C. Through the organization's stock price and market capitalization
  - D. Through the number of employees and their job satisfaction

**Answer Key:**

- 1. C
- 2. D
- 3. A
- 4. B
- 5. A
- 6. C
- 7. B
- 8. D
- 9. FALSE
- 10. A

oceg

