Ultimate Guide to CGRC Certification

Prepare for CGRC with domain insights and test strategies

Arun Kumar Chaudhary

www.bpbonline.com

First Edition 2025

ISBN: 978-93-65894-851

LIMITS OF LIABILITY AND DISCLAIMER OF WARRANTY

The information contained in this book is true and correct to the best of author's and publisher's knowledge. The author has made every effort to ensure the accuracy of these publications, but the publisher cannot be held responsible for any loss or damage arising from any information in this book.

All trademarks referred to in the book are acknowledged as properties of their respective owners but BPB Publications cannot guarantee the accuracy of this information.

Dedicated to

My mom, wife, and daughter

About the Author

Arun Kumar Chaudhary is a highly accomplished and seasoned professional with over 14 years of experience in information security, risk management, and compliance. He holds a master's degree in communication engineering (EEE) from Nanyang Technological University (NTU) and a diploma in cyber law from the Asian School of Cyber Laws. He has extensive expertise in cybersecurity, cloud security, application security, data security, data privacy, risk, and governance. He has actively contributed to ISACA by writing exam questions and remains an engaged member of ISS2 and ISACA. Arun is a prominent speaker at leading cybersecurity conferences and has a proven track record in developing security policies, procedures, and providing internal staff training.

Arun is passionate about improving cybersecurity practices and educating others through his writing and consulting work. He is committed to helping organizations navigate the ever-evolving landscape of information security and privacy. His strong academic background, coupled with his passion for teaching, allows him to effectively engage with students and facilitate their understanding.

He has the following certifications: CISSP, CCSP, CRISC, CISA, CISM, CDPSE, CEH, COBIT 2019, CPFA, LA ISO 27001, LA ISO 42001, CGDPR, ITIL.

About the Reviewers

- **Deepu Thomas** is an information security professional with 20 years of experience, spanning roles as a practitioner, consultant, and trainer. He has worked with organizations across industries, helping them enhance their security posture and achieve compliance with industry standards.

  As an experienced instructor, Deepu delivers certification training for globally recognized bodies such as ISC2 and ISACA, with a focus on information security management. He is passionate about empowering learners, ensuring they gain both knowledge and practical insights to excel in their careers.

  Deepu currently serves as a corporate trainer at Koenig Solutions Pvt. Ltd.

- **Sandeep Sehgal** is a seasoned professional with over 18 years of experience in cybersecurity training, governance, risk, and compliance. He has led numerous awareness programs and policy initiatives to strengthen organizational security postures. His expertise extends to cloud security, where he has worked extensively on implementing secure architectures and mitigating risks across platforms. Recently, Sandeep has been at the forefront of AI compliance and process automation, helping businesses align with emerging regulatory standards. He is a certified cybersecurity professional and holds a master's degree in computer science. Sandeep combines technical expertise with strategic vision to drive secure digital transformation and foster a culture of security and innovation.

- **Saurabh Garg** is a passionate cybersecurity practitioner with extensive experience across security domains, including **Governance, Risk, and Compliance** (**GRC**), cloud security, data protection, and infrastructure security. As a seasoned security architect, he specialises in designing robust security controls and solutions for multinational enterprises.

  Holding industry-leading certifications such as CGRC, CISSP, CCSP, CIPP/E, CISM, CISA and ISO 27001, Saurabh brings deep expertise in helping organisations assess and enhance their IT security posture. In addition to his architecture skills, he has worked as a security presales and transformation consultant with leading **global system integrators** (**GSIs**), enabling businesses to strengthen their cybersecurity strategies effectively.

Acknowledgement

First and foremost, I would like to express my sincere thanks to all those who contributed to the completion of this book. I would like to extend my heartfelt gratitude to my family and friends for their continuous support and encouragement throughout this journey. Their dedication, expertise, and commitment were instrumental and have been a constant source of motivation.

I would also like to extend my appreciation to my mentors and colleagues who provided insight and feedback in polishing the content and enhancing the quality of this book. I would like to express special thanks to my lovely wife **Priya** and my little daughter **Alaya**, who are an integral part of my life and have inspired me to complete this book.

Furthermore, I am extremely grateful to BPB Publications for their guidance and expertise in achieving the completion of this book. Their support and assistance were invaluable in navigating the complexities and overcoming the challenges of the publishing process.

I would also like to acknowledge the support of technical reviewers and editors who provided constructive feedback and contributed to the refinement of this manuscript. Their insights and suggestions have significantly improved the quality of the book. Last but not least, I want to express my thanks to the readers who have shown interest in my book. Your support and encouragement have been deeply appreciated.

Thank you to everyone who participated in making this book a reality.

Preface

In today's fast-paced and ever-changing business environment, the landscape of regulatory compliance is continuously evolving. This is mostly influenced by advancements in technology, global economic changes, and the increasing complexity of business operations. As a result, the need for effective governance, risk management, and compliance practices has become more significant. This book discusses the major areas of GRC, seeking to navigate today's business challenges with clarity and confidence.

This book aims to provide a comprehensive knowledge of GRC principles, which offers an understanding of how organizations can govern risk, ensure compliance, and establish good governance frameworks. It contains immense knowledge and real-world examples to navigate the challenges and opportunities within the GRC domain and will help beginners and experienced professionals to gain knowledge and bring their capabilities to the next level.

It comprises 21 insightful chapters with a wide range of topics essential for understanding the complexities of GRC. This book starts with the introduction of security principles, governance structure and compliance standards providing a solid foundation of basics. From there, we explore the system categorization, control selections, control assessments and enhancing security controls to understand in-depth.

Through practical examples, comprehensive explanations, and a structured approach, this book aims to equip readers with a solid understanding of GRC. The purpose is to adequately prepare you to get certified in GRC. This book serves as a reliable reference for aspiring risk professionals and leaders to expand their knowledge in risk management and industry best practices. Professionals will gain considerable insights into the principles of privacy framework, risk assessment, risk management, and risk treatment.

Chapter 1: Introduction to Security and Privacy Principles - This chapter describes the fundamentals of security principles, including confidentiality, integrity and availability. It provide key security concepts like identification, authentication and authorization essential to drive the security, risk and compliance program. This chapter focuses on data lifecycles, security policy, security principles and roles and responsibilities.

Chapter 2: Governance Structure and Policy - This chapter outlines the organizational framework, including committees and reporting lines, that supports effective oversight and management. Clearly defined roles and responsibilities specify the duties and

accountabilities of individuals and groups, delineating who is responsible for governance, decision-making, and adherence to policies. This chapter also focuses on NIST and the governance framework.

Chapter 3: Risk Assessment and Compliance Standards - This chapter highlights risk analysis to identify and assess potential risk, evaluate their likelihood and impact to prioritize risk effectively. This chapter also defines the requirements and guidelines that organizations must follow to ensure adherence to regulatory and industry-specific requirements.

Chapter 4: Introduction to System Scope - This chapter describes the system purpose and functionality that outlines the primary reason or need for the system. This chapter also specify the limits of the system, identifying what is within its scope and what is external. This chapter also outlines the information types and system boundaries, defining stakeholders and system requirements based on the scope identified.

Chapter 5: System Categorization and Control - This chapter outlines the applicable baseline and inherited controls along with comprehensive understanding of the system's environment. This chapter outlines FIPS 199 and 200 to help organizations determine security controls based on data types and impact levels. This chapter also assesses the effects that changes or events might have on the system's performance, security, and compliance. This chapter also focuses on data privacy standards and personal information.

Chapter 6: Introduction to Control Selection and Approval - This chapter describes the various control framework, including CIS Benchmark, Singapore PDPA and AICPA. It defines security controls based on their purpose and function, such as preventive, detective, and corrective controls, to systematically address different aspects of risk management. This chapter also focuses on privacy assessment to analyze privacy risks.

Chapter 7: Evaluating and Selecting Controls - This chapter outlines the details about customizing security controls to fit the specific needs and risks of an organization, adapting generic controls to align with the particular context. This chapter also define alternative measure implemented when standard controls cannot be applied. This chapter also describes assurance, trustworthiness and focus on creating overlays and system of record notice.

Chapter 8: Enhancing Security Controls - This chapter determine appropriate control enhancements (e.g., security practices, overlays, mitigating controls) and explain metrics used to monitor and evaluate risk levels and performance. This chapter outlines the audit strategies to comply with regulations and overall effectiveness of controls. This chapter also covers the vulnerability management and performance monitoring.

Chapter 9: Introduction to Implementing Controls - This chapter identifies control types (e.g., management, technical, common, operational control) and control implementation aligned with organizational expectations and compliance. **plan of action and milestones** (**POA&M**) defines the plan of action and outlines the specific actions required to address issues, assigns responsibilities, and tracks progress. This chapter also focuses on configuration identification to provide insight into the management of configurations.

Chapter 10: Deploying Security and Privacy Controls - This chapter outlines the control implementation consistent with compliance requirements and identifies the compensating controls. It also covers configuration management to track changes effectively and privacy control guidelines to safeguard personal information and ensuring compliance with privacy laws and regulations.

Chapter 11: Documenting Security Controls - This chapter provides a detailed overview of risk governance to ensure risks are continuously assessed and addressed, and outlines risk register details to track and manage identified risks. This includes residual security risk or planned implementations documentation (e.g., POA&M, risk register).

Chapter 12: Introduction to Control Assessment and Audit - This chapter outlines the assessment objectives, scope, resources, schedule and deliverables. This chapter also covers the techniques and procedures used to carry out an assessment, including interviews, surveys, document reviews. This chapter includes stakeholder roles and responsibilities along with detailed audit scope identified and how evidence can be gathered as per standard.

Chapter 13: Conducting Assessment and Audit - This chapter describes the evaluation of security and privacy controls to determine the effectiveness of controls, ensuring compliance with policies and regulations. It also covers the method used to conduct audits, including the processes, tools, and techniques employed to review compliance. This chapter helps to verify and validate the evidence as part of the audit process.

Chapter 14: Developing Report and Risk Response - This chapter covers the identified risk and risk response (e.g., avoid, accept, share, mitigate, transfer) based on identified vulnerabilities. It highlights the risk management strategy to summarize the risk mitigation plan and register the residual risk based on the risk appetite. This chapter also covers non-compliant findings with newly applied corrective actions reassessed and validated.

Chapter 15: Introduction to System Compliance - This chapter describes how an organization adheres to regulatory requirements, standards, and internal policies. This chapter also outlines the security and privacy documents required to support a compliance decision by the appropriate party (e.g., authorizing official, third-party assessment organizations) compiled, reviewed, and submitted. This chapter also includes disaster recovery plans, backup strategies, and continuity measures to minimize downtime and data loss.

Chapter 16: Determining System Risk Posture - This chapter outlines system risk acceptance criteria, residual risk criteria, and stakeholder concurrence for risk treatments. It covers the overview of an organization's risk landscape, including the identification and assessment of various risks, and the potential impact. The chapter includes test cases, resources required, and criteria for success to ensure the system meets its requirements and operates as intended.

Chapter 17: Documenting System Compliance - This chapter describes the system authorization documentation that provides reliable evidence of the system's security controls. This also includes the formal notification process and documentation related to the findings of an audit conducted on a system. This chapter also covers the training activities, including details on the training programs, participants, completion dates, and effectiveness evaluations. We focus on configuration management minimize security risks.

Chapter 18: Introduction to Compliance Maintenance - This chapter covers the change management process, including planning, approving, implementing, and reviewing changes to minimize the impact on organizational risk, operations, and compliance requirements. It describes the importance of acceptance testing as per the stakeholder's requirements. This chapter also covers the incident response to identify the incident, containing its impact, eradicating the cause, recovering affected systems, and learning from the event to improve future responses.

Chapter 19: Monitoring Compliance - This chapter covers the compliance measurement process for ongoing compliance activities review with stakeholders, as well as system and assets monitoring (e.g., physical and logical assets, personnel, change control). We outline the routine updates, patches, repairs, and performance monitoring to address issues, improve functionality, and ensure that the system continues to meet operational and security requirements. This chapter also focuses on key compliance standards to manage risk and establish organizational governance.

Chapter 20: Optimizing Risk and Compliance - This chapter covers continuous monitoring, testing, and documentation updates (e.g., service level agreements, third-party contracts, policies, procedures). It also focuses on configuration scanning to identify and manage vulnerabilities. This chapter describes the modified monitoring strategies based on updates to legal, regulatory, supplier, security, and privacy requirements.

Chapter 21: Practice Tests - This chapter covers 2 practice tests to evaluate the readiness and preparation for the CGRC exam. There are 50 questions in each practice test covering all the topics, core concepts and knowledge.

Coloured Images

Please follow the link to download the
Coloured Images of the book:

https://rebrand.ly/4vqpnk2

We have code bundles from our rich catalogue of books and videos available at **https://github.com/bpbpublications**. Check them out!

Errata

We take immense pride in our work at BPB Publications and follow best practices to ensure the accuracy of our content to provide with an indulging reading experience to our subscribers. Our readers are our mirrors, and we use their inputs to reflect and improve upon human errors, if any, that may have occurred during the publishing processes involved. To let us maintain the quality and help us reach out to any readers who might be having difficulties due to any unforeseen errors, please write to us at :

errata@bpbonline.com

Your support, suggestions and feedbacks are highly appreciated by the BPB Publications' Family.

Piracy

If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at **business@bpbonline.com** with a link to the material.

If you are interested in becoming an author

If there is a topic that you have expertise in, and you are interested in either writing or contributing to a book, please visit **www.bpbonline.com**. We have worked with thousands of developers and tech professionals, just like you, to help them share their insights with the global tech community. You can make a general application, apply for a specific hot topic that we are recruiting an author for, or submit your own idea.

Reviews

Please leave a review. Once you have read and used this book, why not leave a review on the site that you purchased it from? Potential readers can then see and use your unbiased opinion to make purchase decisions. We at BPB can understand what you think about our products, and our authors can see your feedback on their book. Thank you!

For more information about BPB, please visit **www.bpbonline.com**.

Join our book's Discord space

Join the book's Discord Workspace for Latest updates, Offers, Tech happenings around the world, New Release and Sessions with the Authors:

https://discord.bpbonline.com

Table of Contents

Chapter 1

Introduction to Security and Privacy Principles

Introduction

This chapter provides an overview of essential security concepts needed for understanding how to protect information within an organization. This chapter begins by explaining key security principles, such as **confidentiality, integrity, and availability** (**CIA**), and how these principles guide the development and maintenance of secure systems. This chapter also addresses the importance of data classification and the data lifecycle, which helps in identifying and managing critical assets.

In addition to security principles, the chapter covers the **system development lifecycle** (**SDLC**), detailing how to manage security from both data and system perspectives. It includes discussions on security roles and responsibilities, as well as creating a system threat model. It concludes with a focus on data privacy principles and core components. This chapter also includes practical examples and keynotes to help with understanding and exams.

Structure

The chapter covers the following topics:

- Security principles
- Fundamental security concept

- System development lifecycle
- Data classification and data lifecycle
- Security standards and procedures
- Security roles and responsibilities
- Threat modeling
- Data privacy

Objectives

By the end of this chapter, you will understand the core concept of security. You will be familiar with the security terms and terminology used in an organization. You will gain the key learnings on security principles, security roles and responsibilities, security policies, threat models, and data privacy. You will learn about the data classification and full lifecycleof data.

Security principles

CIA are the core elements of security principles to ensure that the information systems and data are protected from various threats. Together, these security principles help create a robust security framework that protects the data from unauthorized access, ensures its accuracy, and keeps it accessible to those who need it. These security principles are also called the CIA triad, needed for a secure environment. Let us understand the security principle in detail. *Figure 1.1* shows how data is protected with CIA:

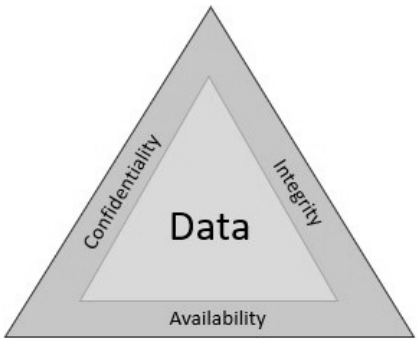

***Figure 1.1**: CIA triad*

Confidentiality

Confidentiality means to protect the system or data from any unauthorized access. The users can intentionally or unintentionally disclose sensitive data if the right security measures are not in place. There are multiple security measures that can be implemented

to ensure the confidentiality of data; however, it is crucial to classify data properly. The security measures can include encryption at rest and in motion, **role-based access control** (**RBAC**), and data classification.

The following provides a list of some controls and how they map to the components of the confidentiality:

- **Encryption of data at rest**: This ensures that stored data is protected from unauthorized access by making it unreadable unless decrypted by authorized users.
- **Encryption of data in transit**: This secures data being transmitted over networks, preventing interception or eavesdropping by encrypting the data during transfer.
- **Encryption of data in use**: This protects data while it is being processed in memory or during active operations, ensuring confidentiality even when the data is not stored or in transit.
- **Access control**: Access control limits access to sensitive data based on user roles and permissions, ensuring only authorized users can access or modify confidential information.

Integrity

Integrity means to protect the system or data from any unauthorized modification. The users can modify the data, resulting in corrupt or non-reliable data if the right security measures are not in place. The data can be corrupted by running malicious codes in the system, inserting incorrect values in the application, deleting configuration files, etc. The security measures can include strict access control, hashing, validating application inputs and intrusion detection.

The following provides a list of some controls and how they map to the components of the integrity:

- **Hashing**: Hashing ensures data integrity by generating a unique hash value for data. Any alteration in the data will change the hash, allowing detection of unauthorized changes.
- **Digital signing**: Digital signature verifies the authenticity and integrity of software or documents by signing them with a private key.
- **Configuration management**: This maintains consistent and authorized configurations for systems and software. It ensures that any changes to the configuration are tracked and authorized.
- **Change control**: Change control manages and tracks changes to systems, applications, and data. It ensures changes are reviewed, tested, and documented to prevent unauthorized modifications.

Availability

Availability means to keep the system up and keep data available in a timely manner to authorized users. Users can sometimes face disruption to the system or connectivity loss if there is no redundancy to the system or network. The disruptions can occur in various ways, like natural disasters, network outages, connectivity loss, application failure, etc. Security measures can include preventing **denial of service** (**DoS**) attacks, redundancy for critical systems, and maintenance of backup systems.

The following provides a list of some controls and how they map to the components of the availability:

- **Clustering**: Clustering ensures system availability by grouping multiple servers to work together. If one server fails, another takes over and minimize downtime.
- **Load balancing**: Load balancers distribute network traffic across multiple servers, preventing any single server from becoming overwhelmed and improving availability by ensuring even workload distribution.
- **Data backups**: Regular backups ensure that data can be restored in the event of system failure or data loss, ensuring continued availability and quick recovery.
- **Failover configurations**: Failover configurations automatically switch to a backup system or component when a failure is detected, maintaining system uptime and availability without manual intervention.
- **Rollback functions**: Rollback allows systems to revert to a previous stable state after an error or failure, minimizing downtime and ensuring continued availability.

Practical illustration

Let us take an example of a health application. You have installed a health application with credentials and you are the authorized user. The hospital uploaded your health records into the application for you to access the information anytime. You do not want anyone to access your health records and hence the application will encrypt your data to prevent it from unauthorized access. This is an example of confidentiality.

You will notice that the application uses digital signatures to verify that the health records have not been modified while sending you in the application. You want to make sure that no one has changed any content of your health records and that the data is accurate. This is an example of integrity.

Let us continue with the same application. You want to have continuous access to the health records available in the application. At the backend, the application maintains multiple servers and data backups to ensure that the application is up always. This is an example of availability.

Fundamental security concept

Authentication, authorization, and accounting (**AAA**) services. This includes implementing authentication protocols, managing user permissions, and tracking activities for compliance and security.

Authentication

Authentication is the initial step in the security process where a user or system proves their identity before gaining access to resources or services. Most of the time, you use a password or a **personal identification number** (**PIN**) to log into any applications or access any system. Authentication can be much more effective with the combinations of various methods, like password and code, sent on registered mobile phone, password and fingerprint, etc. When two or more methods are combined, it is called **multi-factor authentication** (**MFA**) or **two-factor authentication** (**2FA**).

Key aspects of authentication

There are four common methods of authentication: Knowledge, possession, biometrics, and location, explained in the following table:

Method of authentication	Description
Something you know	This is knowledge-based, something you remember or have noted down somewhere. The examples are passwords, PINs, answer to security questions, etc.
Something you have	This is possession-based, something that you hold physically. The examples are smart cards, hardware tokens, **one-time password** (**OTP**) received in mobile phone, etc.
Something you are	This is biometric-based, something that represents the unique characteristic of yourself. The examples are fingerprints, iris scan, etc.
Somewhere you are	This is location-based, something that identifies the user's geographic locations. The examples are IP address, geofencing, etc.

***Table 1.1**: Authentication methods*

There are three main authentication protocols to govern the authentication process explained in the following table: