EDUSUM

#1 Online Certification Guide

GIAC GCIP

GIAC GIAC Critical Infrastructure Protection Certification Questions & Answers

Exam Summary – Syllabus –Questions

GCIP

GIAC Critical Infrastructure Protection

75 Questions Exam – 70% Cut Score – Duration of 180 minutes

Table of Contents:

Know Your GCIP Certification Well:

The GCIP is best suitable for candidates who want to gain knowledge in the GIAC Industrial Control Systems Security. Before you start your GCIP preparation you may struggle to get all the crucial GIAC Critical Infrastructure Protection materials like GCIP syllabus, sample questions, study guide.

But don't worry the GCIP PDF is here to help you prepare in a stress free manner. The PDF is a combination of all your queries like-

- What is in the GCIP syllabus?
- How many questions are there in the GCIP exam?
- Which Practice test would help me to pass the GCIP exam at the first attempt?

Passing the GCIP exam makes you GIAC Critical Infrastructure Protection. Having the GIAC Critical Infrastructure Protection certification opens multiple opportunities for you. You can grab a new job, get a higher salary or simply get recognition within your current organization.

GCIP GIAC Critical Infrastructure Protection Certification Details:

Exam Name	GIAC Critical Infrastructure Protection (GCIP)
Exam Code	GCIP
Exam Price	$979 (USD)
Duration	180 mins
Number of Questions	75
Passing Score	70%
Books / Training	**ICS456: Essentials for NERC Critical Infrastructure Protection**
Schedule Exam	**Pearson VUE**
Sample Questions	**GIAC GCIP Sample Questions**
Practice Exam	**GIAC GCIP Certification Practice Exam**

GCIP Syllabus:

Topic	Details
BES Cyber System Categorization	- Knowledge of Attachment 1 Criteria, Operational Effects and Impacts, NERC Functional Model, BES Reliability Operating Services, BES Cyber Asset Identification
Configuration Change Management and Vulnerability Assessments	- Knowledge of Change Management, Configuration Monitoring, Vulnerability Assessment, Transient Cyber Assets, Removable Media
Electronic Security Perimeter(s)	- Knowledge of Electronic Security Perimeter Architecture, External Routable Connectivity communication, Access Rules, Dial-Up, Malicious Communication Detection, Intermediate Systems and Interactive Remote Access, Multi-factor Authentication
Incident Reporting and Response Planning	- Knowledge of Incident Response Plan, Incident Response Plan Testing and Exercise, Incident Response Plan Reporting
Information Protection	- Knowledge of Information Protection Program, Identification, Classification, Protection, Disposal, Reuse
NERC CIP Terms and Definitions	- Knowledge of terms and definitions relevant to BES, NERC, and CIP
Personnel & Training	- Knowledge of Awareness Program, Cybersecurity Training Program, Personnel Risk Assessment, Access Management Program
Physical Security of BES Cyber Systems	- Knowledge of Physical Security Plan, Physical access controls, Visitor control program, Maintenance and Testing, Monitoring, Logging and Alerting
Recovery Plans for BES Cyber Systems	- Knowledge of Recovery Plan, Recovery Plan Testing and Exercise, Recovery Plan Reporting
Security Management Controls	- Knowledge of Senior Manager Requirements, Policies, Low facility Requirements
Standards Development	- Knowledge of Compliance Monitoring and Enforcement Program, Request For Interpretation, Standards Authorization Request, Urgent Action Request, Balloting, Violation Severity Level, Violation Risk Factor
Standards Enforcement	- Knowledge of Audit Prep, Enforcement Treatment, Reliability Standards Auditor Worksheet, Reliability Assurance Initiative, Interactive Remote Access, Internal

Topic	Details
	Controls Evaluation
System Security Management	- Knowledge of Port and Service management, Patch Management, Malicious Code Prevention, System Logging, Authentication Requirements, Account management, Monitoring and Alerting

GIAC GCIP Sample Questions:

Question: 1

Which of the following best describes the purpose of monitoring communications across an Electronic Security Perimeter?

a) To assess the quality of data transmission.
b) To detect potential cybersecurity events.
c) To bill for data usage.
d) To monitor employee productivity.

Answer: b

Question: 2

What is a key benefit of conducting regular vulnerability assessments on BES Cyber Systems?

a) Identifying and addressing security gaps before they can be exploited.
b) Ensuring compliance with international trade regulations.
c) Facilitating faster system upgrades.
d) Reducing the need for user training.

Answer: a

Question: 3

Which of the following are essential aspects to test in a BES Cyber System recovery plan?

a) The catering arrangements for emergency response teams
b) The effectiveness of communication channels during recovery
c) The speed of system restoration and data recovery
d) The adequacy of entertainment facilities for displaced personnel

Answer: b, c

Question: 4

Why is it important to accurately categorize BES Cyber Systems?

a) To streamline employee access.
b) To prioritize systems for maintenance.
c) To facilitate insurance claims.
d) To ensure appropriate protection levels are applied.

Answer: d

Question: 5

How often should vulnerability assessments be conducted on BES Cyber Systems?

a) Only after a security incident.
b) Bi-annually, regardless of external factors.
c) At a frequency determined by the system's risk assessment.
d) Once every five years.

Answer: c

Question: 6

How might a vulnerability in an electronic security perimeter impact a BES Cyber System?

a) Improved system efficiency
b) Increased public awareness
c) Potential unauthorized access
d) Enhanced employee morale

Answer: c

Question: 7

Which term describes the geographic limit within which all BES Cyber Assets must be contained?

a) Controlled Cyber Domain
b) Regulatory Protection Area
c) Security Management Zone
d) Electronic Security Perimeter

Answer: d

Question: 8

Who is typically responsible for categorizing BES Cyber Systems?

a) The local government.
b) Designated personnel familiar with NERC CIP requirements.
c) External auditors during annual reviews.
d) All employees, as part of their regular duties.

Answer: b

Question: 9

Why is it important to perform vulnerability assessments on BES Cyber Systems?

a) To maintain regulatory compliance and system security
b) To ensure cost-effectiveness
c) To enhance staff productivity
d) To promote industry recognition

Answer: a

Question: 10

What is the primary function of an Electronic Security Perimeter (ESP) in BES Cyber Systems?

a) To ensure all communications are encrypted.
b) To control electronic access to BES Cyber Systems.
c) To monitor environmental conditions within critical facilities.
d) To provide a physical barrier around sensitive equipment.

Answer: b

Study Guide to Crack GIAC Critical Infrastructure Protection GCIP Exam:

- Getting details of the GCIP syllabus, is the first step of a study plan. This pdf is going to be of ultimate help. Completion of the syllabus is must to pass the GCIP exam.
- Making a schedule is vital. A structured method of preparation leads to success. A candidate must plan his schedule and follow it rigorously to attain success.
- Joining the GIAC provided training for GCIP exam could be of much help. If there is specific training for the exam, you can discover it from the link above.
- Read from the GCIP sample questions to gain your idea about the actual exam questions. In this PDF useful sample questions are provided to make your exam preparation easy.
- Practicing on GCIP practice tests is must. Continuous practice will make you an expert in all syllabus areas.

Reliable Online Practice Test for GCIP Certification

Make EduSum.com your best friend during your GIAC Critical Infrastructure Protection exam preparation. We provide authentic practice tests for the GCIP exam. Experts design these online practice tests, so we can offer you an exclusive experience of taking the actual GCIP exam. We guarantee you 100% success in your first exam attempt if you continue practicing regularly. Don't bother if you don't get 100% marks in initial practice exam attempts. Just utilize the result section to know your strengths and weaknesses and prepare according to that until you get 100% with our practice tests. Our evaluation makes you confident, and you can score high in the GCIP exam.

Start Online practice of GCIP Exam by visiting URL
https://www.edusum.com/giac/gcip-giac-critical-infrastructure-protection