

# GICSP Answers Real Questions & GICSP Reliable Learning Materials

---

## **SANS GISCP Exam Questions with 100% Correct Answers | Verified | Latest Update**

### **Industrial Control System (ICS) - Correct Answer-**

A device or set of devices that manage commands directs or regulates the behaviour of other devices or system, bridges cyber to physical, a device that can influence the real world

### **Relays - Correct Answer-**

An electrically operated switch. Complicated to configure cumbersome and expensive

### **Pneumatics - Correct Answer-**

The technique of using gases for power transmission.

### **Control Loops - Correct Answer-**

calculating and controlling an environment or process based on feedback.

### **Proportional Integral Derivative (PID) - Correct Answer-**

a control loop feedback mechanism (controller) widely used in industrial control systems. Calculates an error value as the difference between a measured process variable and a desired setpoint.

The Actualtests4sure is a leading platform that is committed to offering make the GIAC Exam Questions preparation simple, smart, and successful. To achieve this objective Actualtests4sure has got the services of experienced and qualified Global Industrial Cyber Security Professional (GICSP) (GICSP) exam trainers. They work together and put all their efforts and ensure the top standard of Actualtests4sure Global Industrial Cyber Security Professional (GICSP) (GICSP) exam dumps all the time.

Being respected and gaining a high social status maybe what you always long for. But if you want to achieve that you must own good abilities and profound knowledge in some certain area. Passing the GICSP certification can prove that and help you realize your goal and if you buy our GICSP Quiz prep you will pass the exam successfully. Our product is compiled by experts and approved by professionals with years of experiences. You can download and try out our latest GICSP quiz torrent freely before your purchase.

[\*\*>> GICSP Answers Real Questions <<\*\*](#)

## **GICSP examination of the latest GIAC certification exam questions and answers**

Are you struggling to prepare GIAC certification GICSP exam? Do you want to achieve the goal of passing GIAC certification GICSP exam as soon as possible? You can choose the training materials provided by Actualtests4sure. If you choose Actualtests4sure, passing GIAC Certification GICSP Exam is no longer a dream.

## GIAC Global Industrial Cyber Security Professional (GICSP) Sample Questions (Q10-Q15):

### NEW QUESTION # 10

Which control helps prevent threats to Integrity?

- A. Logging IDS alerts
- B. Firewall egress filtering
- C. Centralized LDAP authentication
- D. **Implementing digital signatures**

### Answer: D

Explanation:

Integrity in cybersecurity ensures that data and systems are not altered or tampered with in an unauthorized manner. To protect integrity, controls must verify that data originates from a trusted source and has not been changed.

Digital signatures (D) provide cryptographic proof of data origin and integrity by enabling recipients to verify that the data has not been altered since it was signed.

Firewall egress filtering (A) limits outbound traffic but primarily protects confidentiality and availability, not directly integrity.

Logging IDS alerts (B) supports detection and auditing but is reactive rather than preventive.

Centralized LDAP authentication (C) manages user authentication and access control, mainly protecting confidentiality and accountability.

GICSP highlights digital signatures as a core control to maintain data integrity, especially for firmware, configuration files, and critical commands within ICS.

Reference:

GICSP Official Study Guide, Domain: ICS Security Principles

NIST SP 800-82 Rev 2, Section 6.5 (Information Integrity Controls)

GICSP Training on Cryptographic Controls and Data Integrity

### NEW QUESTION # 11

An administrator relaxes the password policy during disaster recovery operations. What is the result of this action?

- A. Negative effect on recovery point objective (RPO)
- B. **Increased risk**
- C. Positive effect on recovery time objective (RTO)
- D. Reduced insurance needs

### Answer: B

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

Relaxing password policies during disaster recovery often leads to increased risk (C) by weakening authentication controls and potentially allowing unauthorized access.

Recovery Point Objective (RPO) (A) relates to data loss tolerance and is unlikely directly affected by password policies.

Recovery Time Objective (RTO) (B) relates to restoration speed, and while relaxed policies may speed access, this is outweighed by security risk.

Reduced insurance needs (D) is not a direct consequence of relaxed security policies.

GICSP stresses that even during emergencies, security controls should be maintained to prevent additional vulnerabilities.

Reference:

GICSP Official Study Guide, Domain: ICS Security Operations & Incident Response NIST SP 800-34 Rev 1 (Contingency Planning)

GICSP Training on Disaster Recovery and Security Risk Management

### NEW QUESTION # 12

Which of the following is typically performed during the Recovery phase of incident response?

- A. Making a forensic image of the system(s) involved in the incident.
- B. Finding the root cause or vector used by the attacker to gain entry and maintain access.
- C. **Patching and configuring systems to meet established secure configuration standards.**

- D. Updating the organization's security policies to prevent future breaches.

**Answer: C**

Explanation:

The Recovery phase in incident response focuses on restoring systems to normal operations and strengthening defenses:

Patching and configuring systems to meet secure standards (B) is a typical recovery activity to prevent recurrence.

Updating security policies (A) is usually part of the Post-Incident Activities or Governance.

Root cause analysis (C) is typically part of the Investigation or Analysis phase.

Forensic imaging (D) is part of the Containment and Eradication phases for evidence preservation.

GICSP aligns recovery activities with system hardening and return to normal operations.

Reference:

GICSP Official Study Guide, Domain: ICS Security Operations & Incident Response NIST SP 800-61 Rev 2 (Incident Handling Guide) GICSP Training on Incident Response Lifecycle

**NEW QUESTION # 13**

What is an output of a Business Impact Analysis?

- A. Calculating the financial impact of a technology failure
- **B. Prioritizing the business's processes**
- C. Determining the maximum time that systems can be offline
- D. Understanding all of the business's technology functions

**Answer: B**

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

A Business Impact Analysis (BIA) primarily produces a prioritization of the business's processes (B) based on their criticality and impact on organizational goals.

While BIAs help understand downtime tolerance (A) and financial impacts (C), prioritization is the core output guiding recovery efforts.

Understanding technology functions (D) is part of broader asset and risk management but not the primary BIA output.

GICSP highlights BIA as essential for aligning ICS recovery priorities with business needs.

Reference:

GICSP Official Study Guide, Domain: ICS Risk Management

NIST SP 800-34 Rev 1 (Contingency Planning Guide)

GICSP Training on Business Impact Analysis

**NEW QUESTION # 14**

Which of the following can an attacker gain by obtaining PLC logic project files for a SCADA system?

- A. Information about operational firewall rulesets
- B. Schedule of vendor product releases
- **C. Details about the network architecture**
- D. Data regarding personnel and hiring practices

**Answer: C**

Explanation:

Comprehensive and Detailed Explanation From Exact Extract:

PLC logic project files contain the source code and configuration used to program a programmable logic controller (PLC). These files often reveal:

Control logic and operational sequences

Network addressing information

Interconnections between devices and systems

Thus, an attacker with access to these files can infer details about the network architecture (B), including how devices communicate, which protocols are used, and possibly the network topology.

Personnel data (A), firewall rulesets (C), and vendor release schedules (D) are not typically stored within PLC logic projects.

The GICSP framework stresses protecting such engineering artifacts because their compromise can provide an attacker with

valuable insight to facilitate targeted attacks on ICS.

## Reference:

GICSP Official Study Guide, Domain: ICS Security Architecture & Design

GICSP Training Modules on PLC Security and Engineering Artifacts Protection NIST SP 800-82 Rev 2, Section 5.6 (System and Communication Protection)

## NEW QUESTION # 15

• • • • •

No doubt the GIAC GICSP certification exam is a challenging exam that always gives a tough time to their candidates. However, with the help of Actualtests4sure GIAC Exam Questions, you can prepare yourself quickly to pass the GIAC GICSP Exam. The Actualtests4sure GIAC GICSP exam dumps are real, valid, and updated Global Industrial Cyber Security Professional (GICSP) (GICSP) practice questions that are ideal study material for quick GIAC GICSP exam dumps preparation.

**GICSP Reliable Learning Materials:** <https://www.actualtests4sure.com/GICSP-test-questions.html>

We constantly improve and update our GICSP study guide and infuse new blood into them according to the development needs of the times and the change of the trend in the industry, GIAC GICSP Answers Real Questions The test files are available in PDF format and can be read and printed at any time, GIAC GICSP Answers Real Questions They all spent 20 to 30 hours on average to practice the test.

In the book, we introduce a tool called Proactive GICSP Answers Real Questions Risk Management, With these kinds of savings, you can only imagine the pressure placed on the supply chain team to determine GICSP Test Discount the new optimal supply chain structure after an acquisition or merger is announced.

## **Get Marvelous GICSP Answers Real Questions and Pass Exam in First Attempt**

We constantly improve and update our GICSP Study Guide and infuse new blood into them according to the development needs of the times and the change of the trend in the industry.

The test files are available in PDF format and can be read and printed at any time. They all spent 20 to 30 hours on average to practice the test. What are you waiting for, just go for our GICSP exam resources.

Owing to its superior quality and the reasonable price, GICSP our Global Industrial Cyber Security Professional (GICSP) exam study guide files have met with warm reception and quick sale in many countries.

