



# 156-315.81<sup>Q&As</sup>

Check Point Certified Security Expert R81

## Pass CheckPoint 156-315.81 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.geekcert.com/156-315-81.html>

100% Passing Guarantee  
100% Money Back Assurance

Following Questions and Answers are all new published by CheckPoint Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers







icons next to them, which indicate that they are being edited by another administrator in another session. The `admin\\` administrator can unlock these rules by right-clicking on them and selecting Unlock from the menu. However, this will discard the changes made by the original administrator who locked them.

---

## QUESTION 2

What is the purpose of the CPCA process?

- A. Monitoring the status of processes.
- B. Sending and receiving logs.
- C. Communication between GUI clients and the SmartCenter server.
- D. Generating and modifying certificates.

Correct Answer: D

The purpose of the CPCA process is to generate and modify certificates for Check Point products and features. CPCA stands for Check Point Certificate Authority and it is responsible for creating and managing certificates for internal communication between Check Point components, such as Security Gateways, Security Management Servers, SmartConsole clients, and OPSEC applications. CPCA also supports external certificate authorities and can import and export certificates from other sources.

---

## QUESTION 3

Which one of the following is NOT a configurable Compliance Regulation?

- A. GLBA
- B. CJIS
- C. SOCI
- D. NCIPA

Correct Answer: C

The Check Point Compliance Blade is a security management tool that monitors the compliance status of the Security Gateways and Security Management Servers with various regulatory standards<sup>1</sup>. The Compliance Blade supports the following regulatory standards<sup>2</sup>: GLBA: The Gramm-Leach-Bliley Act, also known as the Financial Services Modernization Act of 1999, is a US federal law that requires financial institutions to protect the privacy and security of their customers' personal information. CJIS: The Criminal Justice Information Services Division, also known as CJIS, is a division of the US Federal Bureau of Investigation that provides criminal justice information services to law enforcement, national security, and intelligence agencies. CJIS has a set of security policies and requirements that govern the access, use, and protection of the CJIS data. NCIPA: The National Counterintelligence and Security Center Insider Threat Program Maturity Framework, also known as NCIPA, is a US government framework that provides guidance and best practices for establishing and enhancing insider threat programs within federal agencies. NCIPA defines five levels of maturity for insider threat programs, from initial to optimized. SOCI: This is not a valid option for a configurable Compliance Regulation. There is no such regulatory standard with this acronym. However, there is a similar acronym, SOC 2, which stands for Service Organization Control 2, which is a set of standards and criteria for auditing the security, availability, processing integrity, confidentiality, and privacy of service providers that store, process, or transmit customer data<sup>3</sup>. Therefore, the correct answer is C, as SOCI is not a configurable Compliance



Regulation. References: 1: ATRG: Compliance Blade (R80.10 and higher) - Check Point Software 3 2: Check Point R81 - Check Point Software 1 3: SOC 2 Compliance Checklist: What You Need to Know - Varonis

---

#### QUESTION 4

SandBlast Mobile identifies threats in mobile devices by using on-device, network, and cloud-based algorithms and has four dedicated components that constantly work together to protect mobile devices and their data. Which component is NOT part of the SandBlast Mobile solution?

- A. Management Dashboard
- B. Gateway
- C. Personal User Storage
- D. Behavior Risk Engine

Correct Answer: C

SandBlast Mobile has four components: Management Dashboard, Gateway, Behavior Risk Engine, and On-Device Network Protection. Personal User Storage is not part of the SandBlast Mobile solution. References: SandBlast Mobile Architecture

---

#### QUESTION 5

You want to verify if your management server is ready to upgrade to R81.20. What tool could you use in this process?

- A. migrate export
- B. upgrade\_tools verify
- C. pre\_upgrade\_verifier
- D. migrate import

Correct Answer: C

According to the Check Point website, you can use the pre\_upgrade\_verifier tool to verify if your management server is ready to upgrade to R81.20. This tool checks the compatibility of your current configuration and database with the target version, and provides a detailed report of any issues or warnings. The other tools are either used for exporting or importing databases, or not valid tools. References: Upgrade Verification Service

[Latest 156-315.81 Dumps](#)

[156-315.81 PDF Dumps](#)

[156-315.81 Exam Questions](#)