IBM Security Engineer
Study Guide

This study guide will help prepare you for the IBM **Security Engineer** Certification Examination.

What's in the Study Guide

This study guide covers:

- Security and Compliance Monitoring, Logging and Alerting

How to Use this Study Guide

1) **Read the content.**

2) **Take notes.**

3) **Answer practice questions.**

Preparation

Thorough study is essential to a successful outcome on the exam.

- Clear your schedule.
- Find a quiet place to study.
- Focus on the content.

- Open the associated on-line course for reference.
- Locate the Study Guide.
- Download the Study Guide.

- Print a copy of the Study Guide.
- Take notes.

Modules and Objectives

Modules

1. Security and Compliance Monitoring, Logging and Alerting

Objectives

- Explain the main benefits of IBM Cloud Security Insights
- Describe the 4 key IBM Cloud integrated capabilities and 2 key vendor integrations in IBM Cloud Insights
- Describe the process for Enabling Network Insights and Activity Insights
- Manage alerts relating to Security Threats and Compliance
- Explain Compliance monitoring with the Security Compliance center (SCC), the purpose of SCC, and how it enables continuous security and compliance
- Explain the purpose of the Code Risk Analyzer Plug-in for IBM Cloud and how to configure and use it

Module 1: Security and Compliance Monitoring, Logging and Alerting Introduction and Objectives

In Module 1 of the Study Guide the subject matter:

- Explains how to manage configuration of security and compliance solutions on IBM Cloud.

Lessons

- IBM Security and Compliance Center (SCC)
- Managing Security Threats
- Code Risk Analyzer (CRA) Plug-in for IBM Cloud
- Regulatory Compliance and Continuous Monitoring for Financial Institutions
- Module Summary
- Knowledge Check Questions

Objectives

- Explain the main benefits of IBM Cloud Security Insights
- Describe the 4 key IBM Cloud integrated capabilities and 2 key vendor integrations in IBM Cloud Insights
- Describe the process for Enabling Network Insights and Activity Insights
- Manage alerts relating to Security Threats and Compliance
- Explain Compliance monitoring with the Security Compliance center (SCC), the purpose of SCC, and how it enables continuous security and compliance
- Explain the purpose of the Code Risk Analyzer Plug-in for IBM Cloud and how to configure and use it.

Module 1: Security and Compliance Monitoring, Logging and Alerting
IBM Security and Compliance Center (SCC)

What is the IBM Cloud Security and Compliance Center?

The IBM Cloud Security and Compliance Center (SCC) is a security and compliance management platform that provides continuous security and compliance monitoring. Customers can define controls, monitor security and compliance, remediate issues, collect audit evidence, and assess posture.

SCC Configuration Rules

A configuration rule is a JavaScript object notation (JSON) document that defines the configuration of resources. With the SCC, customers can create rules for specific IBM Cloud resource types to govern how cloud resources can be provisioned or configured by defining:

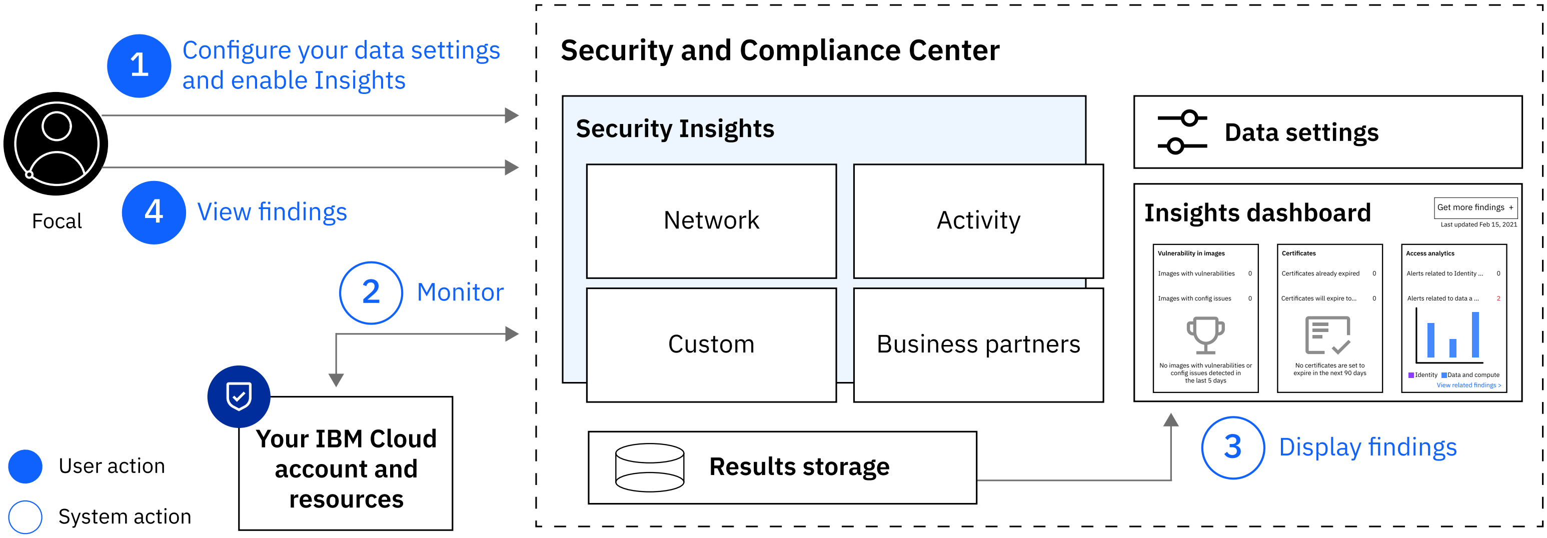
- A target, which may be a workload application.
- The desired configuration rules.
- The enforcement actions the SCC takes if the conditions are not met.

Users can create rules with simple properties, or can build more complex rules with nested properties that contain multiple conditions. An IBM software development kit (SDK) is also available for creating and managing configuration rules in the SCC.

Module 1: Security and Compliance Monitoring, Logging and Alerting
What is Security Insights?

How does Security Insights work?

With Security Insights, you can continuously monitor and analyze your IBM Cloud resources and applications for potential risks that might impact your environment. With Security Insights, you get access to threat detection, security risk prevention, and suggested remediation steps that can help to mitigated issued findings, sent through customized alert notifications, that can give you a more comprehensive understanding of your current security status. Check out the following table to learn more about the different capabilities.


1 Configure your data settings and enable Insights
Focal
4 View findings
2 Monitor
Your IBM Cloud account and resources
User action
System action
Security and Compliance Center
Security Insights
Network
Activity
Custom
Business partners
Data settings
Insights dashboard
Get more findings +
Last updated Feb 15, 2021
Vulnerability in images
Images with vulnerabilities 0
Images with config issues 0
No images with vulnerabilities or config issues detected in the last 5 days
Certificates
Certificates already expired 0
Certificates will expire to... 0
No certificates are set to expire in the next 90 days
Access analytics
Alerts related to Identity ... 0
Alerts related to data a ... 2
Identity
Data and compute
View related findings >
Results storage
3 Display findings

Activity Insights

By comparing user activity that is logged by Activity Tracker against predefined rule packages, you can identify suspicious behavior as it relates to your IBM Cloud resources, which can help to prevent malicious attacks on your applications.

Network Insights

By monitoring and analyzing your VPC flow logs, you can identify suspicious behavior through your the network communication between your VPC interfaces. For example, you can identify Virtual Server Instances that might be compromised or attempts to compromise your VSIs.

Custom insights

To view all of your security alerts in one place, you can integrate your own security tools with the Security and Compliance Center by using the Findings API.

Business partners

If you work with one of our business partners such as Caveonix, Twistlock, or NeuVector, you can easily integrate your findings with the Security and Compliance Center to further assess the risk and compliance posture of your workloads that are deployed on IBM Cloud.

Module 1: Security and Compliance Monitoring, Logging and Alerting
Benefits of Using IBM Cloud Security Insights

Benefits of Using IBM Cloud Security Insights

Security Insights enables customers to better understand their current security status through analysis of their network and activity data. It presents findings on the SCC dashboard. Findings are priority security issues that arise from processing raw events. It also provides:

- Centralized security risk and posture management using a single pane of glass.
- Threat detection and security risk prevention.
- Customized alert notifications that are secured using a private key to encrypt the payload that sends the notification.
- Suggestions for mitigating findings.

Module 1: Security and Compliance Monitoring, Logging and Alerting Endpoint URLS, Authentication and Auditing

Endpoint URLs

SCC supports location-specific endpoint URLs that you can use to interact with the SCC over the public internet. A location represents the geographic area where your SCC requests are handled and processed.

Authentication

Authorization to the SCC API is enforced by using an IBM Cloud Identity and Access Management (IAM) access token. The token is used to determine the actions that a user or service ID has access to when they use the API.

Auditing

You can monitor API activity within your account by using the IBM Cloud Activity Tracker service. Whenever an API method is called, an event is generated that you can then track and audit from within Activity Tracker.

Module 1: Security and Compliance Monitoring, Logging and Alerting
Error Handling

Error handling

SCC uses standard HTTP status codes to indicate whether a method completed successfully. A **200** response always indicates success. A **400** type response is some sort of failure, and a **500** type response usually indicates an internal system error.

Status Code Summary:

Status code	Description
200OK	Everything worked as expected.
201OK	Everything worked as expected. No content is returned.
400Bad Request	The request was unsuccessful, often due to a missing required parameter.
401Unauthorized	The parameters were valid but the request failed due to insufficient permissions.
404Not Found	The requested resource doesn't exist.
409Conflict	The requested resource conflicts with an already existing resource.
410Gone	The requested resource was deleted and no longer exists.
429Too Many Requests	Too many requests hit the API too quickly.
500Internal Server Error	Something went wrong on Security and Compliance Center's end.

Enabling Network Insights

With Security Insights, you can continuously analyze your Virtual Private Cloud (VPC) network interface flow logs to detect any suspicious activity by using learned patterns and threat intelligence.

Before you begin

Before you get started, be sure that you have the required level of access to view and manage Activity Insights. To manage Activity Insights, you must have the Writer service role or higher for Security Advisor and Virtual Private Cloud. You must also have an instance of VPC.

Connecting to Cloud Object Storage

Before you can analyze your network communication, Security Advisor must have access to your network flow logs that are stored in Cloud Object Storage. To create the connection between the services, you must store the logs in a Cloud Object Storage bucket and then grant the service access to the bucket.

Collecting your flow logs

Before it can be analyzed, you must collect your data. To do so, you can create a flow log that collects your network interface logs and funnels them into a Cloud Object Storage bucket.

Enabling analysis

Now that you've connected your Cloud Object Storage bucket and verified that your flow logs are being stored correctly, you can enable Network Insights to start analyzing them.

Available Activity Insights Rule Packages

Rule packages contain rules that are relevant to their specified use. For example, the rules in the App ID rule package help users manage authentication and authorization of applications.

Rule packages are available in Activity Insights for the following services:

- APP ID
- Certificate Manager
- Cloud Databases
- IBM Cloud Object Storage (COS)
- Cloud Shell
- Classic Infrastructure
- IAM
- Key Protect
- Kubernetes Service

Module 1: Security and Compliance Monitoring, Logging and Alerting
Code Risk Analyzer (CRA) Plug-in for IBM Cloud

Code Risk Analyzer (CRA) Plug-in for IBM Cloud

The Code Risk Analyzer (CRA) plug-in enables developers to quickly assess and remediate security and legal risks that they are potentially introducing into source code. It provides feedback directly in Git by posting comments in Git pull requests. CRA is provided as a set of Tekton tasks, and can be easily incorporated into delivery pipelines.

Supported Content

CRA enables discovery of vulnerabilities in the following language and content types:

Content	Description
Java	The repo must use Maven. Dependencies are calculated by using the pom.xml file.
Node.js	Dependencies are calculated by using the package-lock.json file.
Python	Dependencies are calculated by using the requirements.txt file.
Dockerfiles	Files with the Dockerfile pattern in the repo are considered. For container images, the Debian, Red Hat Enterprise Linux, Alpine, and Ubutu Linux distros are supported.
Kubernetes	Files that are suffixed with .yaml and .yml are considered. The kind value must be set to Pod, ReplicaSet, ReplicationController, Deployment, Daemonset, Statefulset, Job, or CronJob.
Terraform	The repo must use Terraform v0.13.5 and IBM Cloud as a Terraform provider for compliance checks.
Golang	Supports go mod and go dep dependency management. For go mod, the go.sum file must be in the repo. For go dep, the Gopkg.lock file must be in the repo.

Module 1: Security and Compliance Monitoring, Logging and Alerting Regulatory Compliance and Continuous Monitoring for Financial Institutions

Overview

As IBM Cloud customers have a variety of compliance requirements, it's important to streamline and support regulated workloads. The IBM approach to managing security and regulatory compliance for financial institutions includes the following two aspects:

1. IBM Cloud Policy Framework for Financial Services

- The IBM Cloud Policy Framework for Financial Services is a set of cloud security and compliance control requirements used as the basis of the IBM policy framework, allowing financial institutions to confidently host key applications and workloads. The IBM Cloud Policy Framework for Financial Services delivers the industry-informed IBM public cloud controls required to operate securely with bank-sensitive data in the public cloud.
- The controls are standardized based on the National Institute of Standards and Technology (NIST) 800-53 control set.

2. SCC

- Enterprises can define controls, assess posture, monitor security and compliance, remediate issues, and collect audit evidence. For example, an enterprise may define a collection of controls (e.g., ‘sensitive workload profile’) to address the security and compliance requirements for a cloud native application that handles sensitive data. These controls can cut across data security, network protection, identity and access management, application security, and audit logging.

Module 1: Security and Compliance Monitoring, Logging and Alerting Summary

Module Summary

- The IBM Cloud Security and Compliance Center (SCC) is a security and compliance management platform that provides continuous security and compliance monitoring.
- With Security Insights, you can continuously monitor and analyze your IBM Cloud resources and applications for potential risks that might impact your environment.
- Security Insights enables customers to better understand their current security status through analysis of their network and activity data. It presents findings on the SCC dashboard. Findings are priority security issues that arise from processing raw events.
- Security and Compliance Center supports location-specific endpoint URLs that you can use to interact with the Security and Compliance Center over the public internet. A location represents the geographic area where your Security and Compliance Center requests are handled and processed.
- Security and Compliance Center uses standard HTTP status codes to indicate whether a method completed successfully. A **200** response always indicates success. A **400** type response is some sort of failure, and a **500** type response usually indicates an internal system error.
- With Security Insights, formerly known as IBM Cloud® Security Advisor, you can continuously analyze your Virtual Private Cloud (VPC) network interface flow logs to detect any suspicious activity by using learned patterns and threat intelligence.
- Rule packages contain rules that are relevant to their specified use. For example, the rules in the App ID rule package help users manage authentication and authorization of applications.
- The Code Risk Analyzer (CRA) plug-in enables developers to quickly assess and remediate security and legal risks that they are potentially introducing into source code.
- As IBM Cloud customers have a variety of compliance requirements, it's important to streamline and support regulated workloads.

Module 1
Check Your Knowledge

Question 1.

What kinds of properties can users create SCC Configuration Rules with? Select all that apply.

A. Simple properties

B. Complex properties

C. Nested properties

D. Small properties

→ Answer A and C. Users can create rules with simple properties, or can build more complex rules with nested properties that contain multiple conditions.

Module 1
Check Your Knowledge

Question 2.

With Security Insights, what do you get access to that can help give you a more comprehensive understanding of your current security status? Select all that apply.

A. Block Storage

B. Security risk prevention

C. VMware vSAN

D. Threat detection

➞ Answer B and D. With Security Insights, you get access to threat detection, security risk prevention, and suggested remediation steps that can help to mitigated issued findings, sent through customized alert notifications, that can give you a more comprehensive understanding of your current security status.

Module 1
Check Your Knowledge

Question 3.

Where does Security Insights present its findings for a customer's current security status?

A. Viewer dashboard
B. SCC dashboard
C. Operator dashboard
D. Administrator dashboard

➞ Answer B. It presents findings on the SCC dashboard.

Module 1
Check Your Knowledge

Question 4.

Where does a location-specific endpoint represent for Security and Compliance Center?

A. Geographic area where your SCC requests are handled and processed
B. Geographic area where the customer creates buckets and objects
C. Area of managing all aspects of data storage
D. Area where you can edit buckets and objects

➞ Answer A. A location represents the geographic area where your Security and Compliance Center requests are handled and processed.

Module 1
Check Your Knowledge

Question 5.

Security and Compliance Center uses standard HTTP status codes to indicate whether a method completed successfully. What does a 400 type response indicate?

A. Success

B. An internal system error

C. Some sort of failure

➞ Answer C. A 400 type response is some sort of failure.

Module 1
Check Your Knowledge

Question 6.

What can you do with Security Insights?

A. Erase users from database
B. Continuously analyze your VPC network
C. Access flow log data
D. None of the above

➞ Answer B. With Security Insights, you can continuously analyze your Virtual Private Cloud (VPC) network interface flow logs to detect any suspicious activity by using learned patterns and threat intelligence.

Module 1
Check Your Knowledge

Question 7.

Rule packages contain rules that are relevant to their specified use. For example, the rules in the App ID rule package help users manage what part of applications? Select all that apply.

A. Access
B. Authentication
C. Authorization
D. Data

➞ Answer B and C. For example, the rules in the App ID rule package help users manage authentication and authorization of applications.

Module 1
Check Your Knowledge

Question 8.

Where does the CRA Plug-in for IBM Cloud provide feedback directly in?

A. Git
B. Red Hat OpenShift
C. User profile
D. Kubernetes

➞ Answer A. It provides feedback directly in Git by posting comments in Git pull requests.

Module 1
Check Your Knowledge

Question 9.

How are the IBM Cloud Policy Framework for Financial Services controls standardized?

A. Following the NIST 300-63 control set
B. Following the NIST 800-53 control set
C. Following the NIST 900-53 control set
D. Following the NIST 400-63 control set

➞ Answer B. The controls are standardized based on the National Institute of Standards and Technology (NIST) 800-53 control set.

Module 1
Check Your Knowledge

Question 10.

The IBM approach to managing security and regulatory compliance for financial institutions includes which two aspects?

A. IBM Cloud Policy Framework for Financial Services

B. SCC

C. Red Hat OpenShift

D. Kubernetes

➞ Answer A and B. The IBM approach to managing security and regulatory compliance for financial institutions includes IBM Cloud Policy Framework for Financial Services and SCC.