servicenow

ServiceNow Certified Implementation Specialist – Security Incident Response Exam Specification

Tokyo Release – Updated December 2022

servicenow

Introduction

The ServiceNow Certified Implementation Specialist – Security Incident Response Exam Specification document defines the purpose, audience, testing options, exam content coverage, test framework, and prerequisites to earn the Certified Implementation Specialist – Security Incident Response certification.

Exam Purpose

The Certified Implementation Specialist – Security Incident Response exam certifies that a successful candidate has the skills and essential knowledge to contribute to the configuration, implementation, and maintenance of a ServiceNow Security Incident Response implementation.

Exam Audience

The ServiceNow Certified Implementation Specialist – Security Incident Response exam is available to ServiceNow customers, partners, employees, and others interested in becoming a ServiceNow Certified Implementation Specialist – Security Incident Response.

Exam Preparation

Exam questions are based on official ServiceNow training materials, the ServiceNow Security Incident Response - ServiceNow Docs and the ServiceNow developer site. Study materials posted elsewhere online are not official and should not be used to prepare for the examination.

Recommended ServiceNow Training

ServiceNow recommends the completion of the following prerequisite training course(s) in preparation for the Certified Implementation Specialist – Security Incident Response exam. Information provided in the following ServiceNow training course(s) contain source material for the exam.

- Welcome to ServiceNow
- ServiceNow Administration Fundamentals
- ServiceNow Platform Implementation
- Automated Test Framework Fundamentals
- Flow Designer Essentials
- IntegrationHub Essentials
- Mobile Development Essentials
- Service Portal Fundamentals
- Common Service Data Model Fundamentals
- Configuration Management Database Fundamentals
- Now Experience UI Builder Fundamentals

- Configuration Compliance Essentials
- What's New in the Store for Security Operations

Required ServiceNow Training

ServiceNow requires completion of the following training course(s) and certification(s). The content in these courses covers the exam learning domains and will help you prepare for the exam.

- Security Operations Fundamentals
- Security Incident Response Implementation

Upon completion of the Incident Security Response Implementation course, the candidate will be eligible to obtain or purchase a nontransferable voucher code to register for the Certified Implementation Specialist – Security Incident Response exam.

Additional Resources

In addition to the above, the candidate may find the following additional resources valuable in preparation for the exam.

- Candidate Journey Guide – a resource to guide you through the entire certification process
- Tokyo Security Operations Documentation
- Tokyo Security Incident Response Documentation
- Security Operations Community Forum

Additional Recommended Experience

- Three to six months of field experience participating in a ServiceNow Security Incident Response deployment project or maintaining the Security Incident Response application suite in a ServiceNow instance.
- General familiarity with industry terminology, acronyms, and initialisms.

Exam Scope

Learning domains are the key topics and specific objectives included in the exam. Exam content or exam items are divided into learning domains.

The following table shows the learning domains, weightings, sub-topics, and the percentage of questions represented in each domain. The listed sub-skills should NOT be considered an all-inclusive list of the exam content.

Number of Domains	Learning Domain	Percent of Exam
1	**Security Incident Response Overview and Data Visualization** • Introducing Security Incident Response • Data Visualization • Understanding Customer Goals and Meeting Customer Expectations	15%
2	**Security Incident Creation and Threat Intelligence** • Explore How to Create Security Incidents • Major Security Incident Management • Understanding Threat Intelligence • MITRE ATT&CK Framework	14%
3	**Security Incident and Threat Intelligence Integrations** • ServiceNow Store and Share • Managing Pre-Built Integrations • Creating Custom Integrations	14%
4	**Security Incident Response Management** • Security Analyst Workspace • Standard Automated Assignment Options • Definition of Escalation Paths • Security Tags • Process Definitions and Selection	15%
5	**Risk Calculations and Post Incident Response** • Security Incident Calculator Groups and Risk Scores • Post Incident Reviews	12%
6	**Automation and Standard Processes** • Automate Security Incident Response Overview • Security Incident Automation Using Flows and Workflows	30%

	• Playbook Automation (Knowledge Articles and Runbooks) • Use Case: User Reported Phishing v2	
	Total	100%

Exam Registration

ServiceNow partners with Kryterion using its Webassessor platform for exam registration. Our mainline exams are offered at Kryterion Test Centers or can be taken anywhere online while a Kryterion proctor monitors the exam appointment.

To register for an exam, you will need to create a Webassessor account and then link it to your Now Learning account.

For individuals with a disability or English as Second Language (ESL), ServiceNow does offer reasonable accommodation while taking the certification exam.

Exam Structure

Number of Items

The exam consists of 60 questions.

Multiple Choice (single answer)

For each multiple-choice question on the exam, there are at least four possible responses. Select the one response that most accurately answers the question.

Multiple Select (select all that apply)

For each multiple-select question on the exam, there are at least four possible responses. The question will state how many responses should be selected. Select ALL responses that accurately answer the question. Partial credit is not provided.

Exam Result

The exam result is immediately displayed as a conditional pass or fail result after completing and submitting the exam. Additional scoring information can be found in the Obtain the Exam Result lesson in the Candidate Journey Guide.

Pass Result

A pass result indicates that the certification has been earned. The only information shared is the pass result. The pass result is conditional, meaning the exam at any time can be audited, reviewed, and the certification may be revoked after investigation if it is found that the ServiceNow Test Security Policies have been violated.

To maintain a ServiceNow Certification, you will need to pass delta exams and pay the annual Certification Maintenance Program (CMP) Fee.

Fail Result

A failed result indicates that the certification was not earned. The percent earned for each learning domain is shared. For the next exam attempt, focus on the learning domains with the lowest percentage scores.

Sample Questions

Sample Item #1

Which role is needed to install the Security Incident Response application?

A. sn_si.admin
B. admin
C. sn_sec_cmn.admin
D. sn_si.write

Correct Answer: B

Sample Item #2:

Security Incident Response can be defined as:

A. The action plan taken to mitigate security incidents and imminent security threats
B. The change plan taken to fulfill requests raised through the Security Incident Catalog
C. The reaction plan taken to capture and record security incidents
D. The response plan taken to react to imminent security threats

Correct Answer: A

Sample Item #3:

In which ServiceNow module can you find pre-built integrations?

A. Integrations
B. Sightings Search Configuration
C. Integration Configurations
D. Integration Status
Correct Answer: C

Sample Item #4:

Which process definition is set as default for security incident response application?

A. NIST Open
B. SANS Open
C. SANS Stateful
D. NIST Stateful

Correct Answer: D

Sample Item #5:

Which of the following statements best describes what Security Incident Calculators are used to do?

A. Set specific values according to matched conditions
B. Determine the Security Incident Risk Score
C. Calculate the cost of an incident
D. Calculate the time spent in the various incident states

Correct Answer: A

Sample Item #6:

A flow executes when what is met?

A. A trigger condition
B. IntegrationHub activation
C. Response Task state is Active
D. NIST Ready State

Correct Answer: A

Sample Item #7:

Identify three key Security Incident Response reporting audiences:

A. Security Analysts
B. Security Managers
C. CIOs/CISOs
D. Facilities Managers
E. Human Resources Managers

Correct Answers: A, B, C