ServiceNow
Certified Implementation Specialist - Security Incident Response
Exam Specification

New York Release – Updated September 4, 2019

Introduction

The ServiceNow Certified Implementation Specialist - Security Incident Response (SIR) Exam Specification defines the purpose, audience, testing options, exam content coverage, test framework, and prerequisites to become a ServiceNow Implementation Specialist for Security Incident Response.

Exam Purpose

The ServiceNow Certified Implementation Specialist 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 employees and ServiceNow partners.

Exam Preparation

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

Prerequisite ServiceNow Training Path

ServiceNow requires 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.

- Security Operations Fundamentals
- Security Incident Response Implementation - *Upon completion, the candidate will be issued a voucher code to register for the Certified Implementation Specialist - Security Incident Response exam.

Recommended Knowledge & Education

ServiceNow recommends completion of the following Training Course(s) and Certification(s) in preparation for the exam.

- Implementation Learning Path
- Certified System Administrator
- Automated Test Framework Fundamentals
- Flow Designer Fundamentals
- IntegrationHub Fundamentals

- Mobile Development Fundamentals
- Service Portal Fundamentals
- Certified Implementation Specialist - ITSM
- ITIL v3 Foundations Certified (Recommended)
- ServiceNow Scripting Fundamentals
- ServiceNow System Administration Advanced

Additional Recommended Experience

- Six (6) months field experience participating in ServiceNow deployment projects or maintaining ServiceNow instances
- Participation in at least two ServiceNow deployment projects
- General familiarity with industry terminology, acronyms, and initialisms

Exam Scope

Exam content is divided into Learning Domains that correspond to key topics and activities typically encountered during ServiceNow implementations. In each Learning Domain, specific learning objectives have been identified and are tested in the exam.

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

	Learning Domain	% of Exam
1	**Security Incident Response Overview**	**10%**
2	**Create Security Incidents**	**20%**
3	**Security Incident Response Management**	**20%**
4	**Post Incident Response**	**20%**
5	**Security Incident Integrations**	**15%**
6	**Automation and Standard Processes**	**10%**
7	**Data Visualization**	**5%**
8	**Madrid Security Incident Response DELTA**	**0%**
9	**Capstone Project**	**0%**
	Total	**100%**

Exam Registration

Each candidate must register for the exam via the ServiceNow Webassessor website using a voucher obtained by completing the Security Incident Response Implementation training prerequisite.

During the registration process, each test taker has the option of taking the exam at an Authorized Testing Center or as an online-proctored exam. In both testing venues, the Certified Implementation Specialist exam is done through a consistent, friendly, user interface customized for ServiceNow tests.

The Kryterion testing network is worldwide and all locations offer a secure, comfortable testing environment. Candidates register for the exam at a specific date and time so there is no waiting and a seat is reserved in the testing center.

Each candidate can also choose to take the exam as an online-proctored exam. This testing environment allows a candidate to take the test on his or her own system provided that certain requirements are met.

NOTE: A special accommodation version of the exam is available. Contact certification@servicenow.com for more information. Depending on the accommodation, there may be a 30-day lead time before testing.

Exam Structure

The exam consists of approximately (60) questions. For each question on the examination, there are multiple possible responses. The person taking the exam reviews the response options and selects the *most correct* answer to the question.

Multiple Choice (single answer)

For each multiple-choice question on the exam, there are at least four possible responses. The candidate taking the exam reviews the response options and selects the one response 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. The candidate taking the exam reviews the response options and selects ALL responses that accurately answer the question. Multiple-select questions have two or more correct responses.

Matching

A matching item requires a test taker to assign listed answer options to a parallel list of queries. The test taker must correctly match all queries to answers in order for the item itself to be judged correct. Up to 20 elements and 20 options can be listed. Partial credit may be given.

Exam Results

After completing and submitting the exam, a pass or fail result is immediately calculated and displayed to the candidate. More detailed results are not provided to the candidate.

Exam Retakes

If a candidate fails to pass an exam, they may register to take the exam again up to three more times for a cost of $75.

Sample Question(s)

Sample Item #1:

David is on the Network team and has been assigned a security incident response task. What role does he need to be able to view and work the task?

A. Security Analyst
B. Read
C. External
D. Security Basic

Answer: C

Sample Item #2:

True or False: Someone with the ITIL role has the ability to raise a Security Incident by using the Create Security Incident button from an incident form.

A. True
B. False

Answer: A

Sample Item #3:

Which of the following State Flows are provided for Security Incidents? (Select all that apply)

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

Answers: A, B, C

Sample Item #4:

Security Calculator groups can be used for which of the following: (Select all that apply)

A. Determining the Risk Score on a Security Incident
B. Setting Priority on a Security Incident
C. Calculating Time to Contain on a Security Incident
D. Setting Business Impact on a Security Incident
E. Answers: B, D

Sample Item #5:

Which of the following is a Security Incident Threat Lookup Integration?

A. Splunk
B. VirusTotal
C. WhoisXML
D. Tanium

Answer: B

Sample Item #6:

A customer has asked you how the Security Admin (someone with the sn_si.admin role) can determine when the Phishing Workflow is launched. How would you instruct them to do it?

A. Edit the conditions on the workflow to launch when the category of the incident is set to Phishing
B. Edit the conditions on the workflow to launch when short description of the incident contains Phishing
C. Set a workflow trigger to execute the workflow when the category is set to Phishing
D. Set a workflow trigger to execute the workflow whenever an email is attached to the incident

Answer: C

Sample Item #7:

Which Table would be commonly used for Security Incident Response?

A. sn_si_incident
B. sec_ops_incident
C. cmdb_rel_ci
D. sysapproval_approver

Answer: A