CertNexus IRBIZ™ (IRZ-110) Exam Blueprint

Date Issued: 7/1/2019
Date Modified: 11/10/2024
Version: 1.0

Introduction to CertNexus

CertNexus is a vendor-neutral certification body, providing emerging technology certifications and micro-credentials for business, data, developer, IT, and security professionals. CertNexus' mission is to assist closing the emerging tech global skills gap while providing individuals with a path towards rewarding careers in Cybersecurity, Data Science, Data Ethics, Internet of Things, and Artificial Intelligence (AI)/ Machine Learning (ML).

We rely on our Subject Matter Experts (SMEs) to provide their industry expertise and help us develop these credentials by participating in a Job Task Analysis, Exam Item Development, and determining the Cut Score. We also depend upon practitioners in the field to participate in a survey of the Job Task Analysis and beta testing to ensure that our certifications validate knowledge and skills relevant to the industry.

Copyright ©2024 by CertNexus Inc. (a division of Logical Operations).
All rights reserved.
CertNexus IRZ-110 Exam objectives are subject to change without notice.

CertNexus IRBIZ™ (IRZ-110) Exam Blueprint

Exam Information

Candidate Eligibility

The IRBIZ assessment requires no application fee, supporting documentation, or other eligibility verification measures for you to be eligible to take it. Simply purchase an access key for the *IRBIZ™ (Exam IRZ-110): Incident Response for Business Professionals* course from the CertNexus Store [here]. This course includes access to the credential process directly through the CHOICE platform.

Exam Prerequisites

Successful candidates should have a fundamental knowledge of business processes and general business concepts, as well as domain knowledge in cybersecurity incident response. It is recommended that candidates acquire domain knowledge by attending the CertNexus® *IRBIZ™ (Exam IRZ-110): Incident Response for Business Professionals* course prior to taking the assessment.

Exam Specifications

Number of Items: 10

Passing Score: 80% or 8/10 items

Duration: Estimated 15–30 minutes; candidates may retake as many times as desired.

Exam Delivery: Online through the CHOICE platform

Item Formats: Multiple Choice/Multiple Response/True–False

Upon successful completion, candidates will earn the CertNexus IRBIZ credential.

Exam Description

Target Audience:
The IRBIZ assessment is primarily designed for IT leaders, consultants, product and project managers, and other decision makers who are responsible for complying with incident response legislation. Other individuals who wish to validate basic incident-response knowledge are also candidates for this assessment.

Exam Objective:
Upon successful completion of the IRBIZ assessment, business professionals will demonstrate an wwwunderstanding of what incident response is, why it's important, how to apply it to the business, and how to fit it into an overall compliance strategy.

Copyright ©2024 by CertNexus Inc. (a division of Logical Operations).
All rights reserved.
CertNexus IRZ-110 Exam objectives are subject to change without notice.

To ensure that candidates possess the aforementioned knowledge, skills, and abilities, the IRBIZ assessment will test them on the following domains with the following weightings:

Domain	% of Examination
1.0 Assess Information Security Risk	30%
2.0 Respond to Cybersecurity Incidents	30%
3.0 Investigate Cybersecurity Incidents	30%
4.0 Comply with Legislation	10%
Total	**100%**

The information that follows is meant to help you prepare for your credential assessment. This information does not represent an exhaustive list of all the concepts and skills that you may be tested on during your assessment. The domains, identified previously and included in the objectives listing, represent the large content areas covered in the assessment. The objectives within those domains represent the specific tasks associated with the job role(s) being tested. The information beyond the domains and objectives is meant to provide examples of the types of concepts, tools, skills, and abilities that relate to the corresponding domains and objectives. All this information represents the industry-expert analysis of the job role(s) related to the credential and does not necessarily correlate one-to-one with the content covered in your training program or on your assessment. We strongly recommend that you study independently to familiarize yourself with any concept identified here that was not explicitly covered in your training program or products.

Domains and Objectives

Domain 1.0 Assess Information Security Risk [30%]

Objective 1.1 Identify the importance of risk management.

- Cybersecurity fundamentals
  - Key terms (assets, threats, attacks, risks, etc.)
  - Risk factors
  - Risk equation
- Risk management
  - Phases of risk management cycle
  - ERM
  - Risk exposure
  - Risk analysis methods
  - Risk types and impacts

Copyright ©2024 by CertNexus Inc. (a division of Logical Operations).
All rights reserved.
CertNexus IRZ-110 Exam objectives are subject to change without notice.

Objective 1.2 Integrate documentation into risk management.

- Document types
  - Policies
  - Standards
  - Guidelines
  - Procedures
- Lifecycles
  - Policy lifecycle
  - Process/procedure lifecycle
- Types of policies
  - Incident response policy
  - Acceptable use policy
  - Password policy
- Types of procedures
  - Evidence production
  - Patching
  - Exception management
- Content of policies/procedures
  - Scope
  - Information classification
  - Consequences
  - Best practices
- Business documents supporting security
  - SOA
  - BIA
  - MOU

Copyright ©2024 by CertNexus Inc. (a division of Logical Operations).
All rights reserved.
CertNexus IRZ-110 Exam objectives are subject to change without notice.

Domain 2.0 Respond to Cybersecurity Incidents [30%]

Objective 2.1 Deploy an incident-handling and response architecture.

- Planning
  - Incident handling and response
  - DRP
- CSIRT
  - Teams
  - Roles
  - SOCs
  - Daily duties
  - External/internal communication
- Incident identification
  - IOCs
  - Impact and scope
- Incident evaluation/analysis
  - Log analysis
  - Baseline comparison
  - Event correlation
- Incident containment/mitigation/eradication
  - Personnel safety
  - Account disabling
  - Network isolation
- Incident recovery
  - Data restoration
  - Health checks
  - Malware removal
- Post-incident
  - AAR/LLR
  - Non-technical analyses
  - Technical analyses
  - Questions that need answering
- Incident-handling tools
  - Drive imagers
  - Network-share enumerators
  - Data recovery software

Copyright ©2024 by CertNexus Inc. (a division of Logical Operations).
All rights reserved.
CertNexus IRZ-110 Exam objectives are subject to change without notice.

Objective 2.2 **Contain and mitigate incidents.**

- Techniques
  - System hardening
  - Blacklisting/whitelisting
  - DNS filtering
  - Black-hole routing
  - Mobile device management
  - Secure erasure/disposal
  - Access control
- Devices and tools used in containment/mitigation
  - Firewalls
  - IDS/IPS
  - Endpoint security
- Case studies
  - Data-breach incident
  - DoS incident
  - APT incident

Objective 2.3 **Prepare for forensic investigation.**

- Forensic analysts
  - Duties
  - Expertise
  - Connection to legal entities
- Communication between CSIR and forensic analysts
  - Communicate incident outcomes
  - Designate liaisons
  - Detail findings
  - Detail handling/recovery actions taken

Domain 3.0 Investigate Cybersecurity Incidents [30%]

Objective 3.1 **Apply a forensic investigation plan.**

- Forensic-analyst tasks
  - Obtain evidence
  - Document evidence
  - Support prosecution
- Forensic investigations
  - Forensic-investigation models
  - Prepare for forensic investigations
  - Adhere to investigation scope
- Forensic techniques
  - Timeline generation/analysis
  - Evidence authentication
  - Chain of custody
- Forensic toolkit
  - Software
  - Physical

Copyright ©2024 by CertNexus Inc. (a division of Logical Operations).
All rights reserved.
CertNexus IRZ-110 Exam objectives are subject to change without notice.

Objective 3.2 **Securely collect and analyze electronic evidence.**

- Order of volatility
  - AM vs. storage drives
- File recovery
  - File systems
  - File carving
  - Data extraction
- Data preservation
  - Evidence backup/replication
  - Secure storage
  - Climate controls
  - Tracking metadata
- Forensic procedures for compromised systems
  - Capture forensic images
  - Examine network traffic/logs
  - Take hashes

Objective 3.3 **Securely collect and analyze electronic evidence.**

- Cyberlaw
  - Identify relevant laws and regulations
  - Rely on legal counsel
- Work with law enforcement
  - Law-enforcement liaisons
  - Technical expertise in legal cases
  - Evidence sharing

Domain 4.0 Comply with Legislation [10%]

Objective 4.1 **Comply with federal and national legislation.**

- Federal laws/regulations
  - SOX
  - HIPAA
  - GDPR
  - Data Protection Act
  - Computer Misuse Act
- GDPR case studies
  - Accountability
  - Notification thresholds
  - Notification content/delivery

Objective 4.2 **Comply with state legislation.**

- State laws/regulations
  - CCPA
  - NYS Information Security Breach and Notification Act
  - Jurisdiction considerations
- State vs. federal law
  - Extensions
  - Exceptions
  - Conflicts

Copyright ©2024 by CertNexus Inc. (a division of Logical Operations).
All rights reserved.
CertNexus IRZ-110 Exam objectives are subject to change without notice.

IRBIZ Acronyms

Acronym	Expanded Form
AI	Artificial intelligence
AAR	After-action report
ACL	Access control list
APT	Advanced persistent threat
BIA	Business impact analysis
BCP	Business continuity plan
BPA	Business partnership agreement
CCPA	California Consumer Privacy Act
CERT	Computer emergency response team
CFAA	Computer Fraud and Abuse Act
CIA	Confidentiality, integrity, availability
CIS	Center for Internet Security
CMIA	Confidentiality of Medical Information Act
CSIRT	Cybersecurity incident response team
DDoS	Distributed denial of service
DoS	Denial of service
ERM	Enterprise risk management
FAT32	File Allocation Table (32 bit)
FISMA	Federal Information Security Management Act
GDPR	General Data Protection Regulation
GLBA	Gramm–Leach–Bliley Act
HFS+	Hierarchical File System Plus
HIDS	Host-based intrusion detection system
HIPAA	Health Insurance Portability and Accountability Act
HIPS	Host-based intrusion prevention system
IA	Interoperability agreement
IDS	Intrusion detection system
IOC	Indicator of compromise

Copyright ©2024 by CertNexus Inc. (a division of Logical Operations).
All rights reserved.
CertNexus IRZ-110 Exam objectives are subject to change without notice.

IoT	Internet of Things
IPS	Intrusion prevention system
ISA	Interconnection security agreement
ISO	International Organization for Standardization
LLR	Lessons-learned report
MAC	Mandatory access control
MDM	Mobile device management
MOU	Memorandum of understanding
MSA	Master service agreement
NAC	Network access control
NDA	Non-disclosure agreement
NIDS	Network intrusion detection system
NIPS	Network intrusion prevention system
NIST	National Institute of Standards and Technology
NTFS	New Technology File System
OLA	Operating-level agreement
OLE	Office of Legal Education
PCI DSS	Payment Card Industry Data Security Standard
PHI	Protected health information
PII	Personally identifiable information
PIPEDA	Personal Information Protection and Electronic Documents Act
RAM	Random-access memory
ReFS	Resilient File System
SIEM	Security information and event management
SLA	Service-level agreement
SOA	Statement of applicability
SOC	Security operations center
SOX	Sarbanes–Oxley Act
TSK	The Sleuth Kit
VM	Virtual machine
VPN	Virtual private network

Copyright ©2024 by CertNexus Inc. (a division of Logical Operations).
All rights reserved.
CertNexus IRZ-110 Exam objectives are subject to change without notice.

CertNexus offers personnel certifications and micro-credentials in a variety of emerging technology skills including Cybersecurity, Cyber Secure Coding, the Internet of Things (IoT), IoT Security, Data Science, Artificial Intelligence, and Data Ethics. For a complete list of our credentials visit **https://certnexus.com/certification/**.

CERTNEXUS®

1150 University Ave, Suite 20, Rochester, NY 14607
1-800-326-8724 | info@certnexus.com
certnexus.com