Certified in Cybersecurity

1. Security Principles
2. Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts
3. Access Controls Concepts
4. Network Security
5. Security Operations

Certified in Cybersecurity Examination Weights

Domains	Average Weight	# of Items
1. Security Principles	26%	20
2. Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts	10%	7
3. Access Controls Concepts	22%	17
4. Network Security	24%	18
5. Security Operations	18%	13
Total	100%	75*

*Each exam also contains 25 pre-test items for a total of **100 items** during the pilot exam. They're included for research purposes only. The pre-test items aren't identified, so answer every item to the best of your ability.

Certified in Cybersecurity Examination Information

Length of exam	2 hours
Number of items	100
Item format	Multiple choice
Passing grade	700 out of 1000 points
Exam language availability	English
Testing center	Pearson VUE Testing Center

Domain 1: Security Principles (26%, 20 items)

1.1 Understand the security concepts of information assurance

- Confidentiality
- Integrity
- Availability
- Authentication (e.g., methods of authentication, multi-factor authentication (MFA))
- Non-repudiation
- Privacy

1.2 Understand the risk management process

- Risk management (e.g., risk priorities, risk tolerance)
- Risk identification, assessment and treatment

1.3 Understand security controls

- Technical controls
- Administrative controls
- Physical controls

1.4 Understand (ISC)^2 Code of Ethics

- Professional code of conduct

1.5 Understand governance processes

- Policies
- Procedures
- Standards
- Regulations and laws

Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts (10%, 7 items)

2.1 Understand business continuity (BC)

- Purpose
- Importance
- Components

2.2 Understand disaster recovery (DR)

- Purpose
- Importance
- Components

2.3 Understand incident response

- Purpose
- Importance
- Components

Domain 3: Access Controls Concepts (22%, 17 items)

3.1 Understand physical access controls

- Physical security controls (e.g., badge systems, gate entry, environmental design)
- Monitoring (e.g., security guards, closed-circuit television (CCTV), alarm systems, logs)
- Authorized versus unauthorized personnel

3.2 Understand logical access controls

- Principle of least privilege
- Segregation of duties
- Discretionary access control (DAC)
- Mandatory access control (MAC)
- Role-based access control (RBAC)

- Domain 4: Network Security (24%, 18 items)
-

4.1 Understand computer networking

- Networks (e.g., Open Systems Interconnection (OSI) model, Transmission Control Protocol/Internet Protocol (TCP/IP) model, Internet Protocol version 4 (IPv4), Internet Protocol version 6 (IPv6), WiFi)
- Ports
- Applications

4.2 Understand network threats and attacks

- Types of threats (e.g., distributed denial-of-service (DDoS), virus, worm, Trojan, man-in-the-middle (MITM), side-channel)
- Identification (e.g., intrusion detection system (IDS), host-based intrusion detection system (HIDS), network intrusion detection system (NIDS))
- Prevention (e.g., antivirus, scans, firewalls, intrusion prevention system (IPS))

4.3 Understand network security infrastructure

- On-premises (e.g., power, data center/closets, Heating, Ventilation, and Air Conditioning (HVAC), environmental, fire suppression, redundancy, memorandum of understanding (MOU)/memorandum of agreement (MOA))
- Design (e.g., network segmentation (demilitarized zone (DMZ), virtual local area network (VLAN), virtual private network (VPN), micro-segmentation), defense in depth, Network Access Control (NAC) (segmentation for embedded systems, Internet of Things (IoT))
- Cloud (e.g., service-level agreement (SLA), managed service provider (MSP), Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), hybrid)

Domain 5: Security Operations (18%, 13 items)

5.1 Understand data security

- Encryption (e.g., symmetric, asymmetric, hashing)
- Data handling (e.g., destruction, retention, classification, labeling)
- Logging and monitoring security events

5.2 Understand system hardening

- Configuration management (e.g., baselines, updates, patches)

5.3 Understand best practice security policies

- Data handling policy
- Password policy
- Acceptable Use Policy (AUP)
- Bring your own device (BYOD) policy
- Change management policy (e.g., documentation, approval, rollback)
- Privacy policy

5.4 Understand security awareness training

- Purpose/concepts (e.g., social engineering, password protection)
- Importance