

1- Security and Risk Management + Data Protection

1. **An organization conducting an ongoing effort to ensure an organizations assets and/or people remain protected is called what?**
Due Dilligence
2. **When determining the value of an organizational asset, which is LEAST important**
How long it will take to replace the asset
3. **If you cannot determine how much a system asset costs, what is the best approach to perform a risk assessment?**
A qualitative risk assessment
4. **Which one of the following is NOT a canon of the COE?**
Always provide the best possible security protection based on your current knowledge and skill level
5. **When deciding to mitigate a security risk, what is the focus of doing this?**
Reducing the risk to an acceptable level
6. **When an organization wants to declare very detailed and short-range security goals and objectives, this should be documented in a:**
Operational Plan
7. **The states of data are comprised of each of these but DOES NOT include this:**
Data in process
8. **Data is MOST vulnerable when it is:**
In transit
9. **Due care can be explained as:**
The reasonable effort to protect an asset
10. **A conceptual formula to calculate a security risk is:**
 $\text{Threats} * \text{Vulnerabilities}$
11. **Michael is a new security engineer working for a small company. He received notification from a firewall vendor stating the operating system had a critical vulnerability and a patch update was available to correct the vulnerability.**
Follow the established security policy for handling patch updates
12. **When performing a cost/benefit analysis, which is NOT a consideration when making a risk based decision?**
Determining how much information to provide senior management so that they can make a decision
13. **How many canons are in the (ISC)2 Code of Ethics (COE)?**
4
14. **As it pertains to information security, availability is important to ensure:**
Data is available for users when they need it
15. **To discover the potential loss for a single security occurence, the proper formula to use is:**
 $\text{AV} * \text{EF}$
16. **An example of a security standard is:**
The requirements to securely configure a software application
17. **What is NOT a common technique to implement confidentiality in an information system?**
Hashing
18. **Least privilege is important to ensure users only have:**
The privilege levels necessary to perform their tasking
19. **High level and long-range security goals should be documented in a:**
Strategic Plan
20. **The purpose of a security policy is NOT to:**
Define a consistent set of actions required to implement security

2-Asset Security + Architecture + Security Engineering

1. **The 3 main categories of security controls are:**

Administrative, physical, and technical

2. **DevOps is the process of combining system development and operations into a continuous process. When assessing the security architecture, what is one of the most important parts of DevOps security?**

Security must be integrated into DevOps as part of system and security architecture

3. **What type of security control is used to address a known risk, vulnerability, or threat that cannot be mitigated directly**

Compensating control

4. **The information system you are working with is referred to as an closed system. Why is it important to know the difference between a closed or open system?**

Closed systems typically create more vulnerabilities due to lack of best practices and standards

5. **When using SHA to hash an input value, what key size would create the STRONGEST encryption?**

512 bits

6. **What kind of system is designed to operate large scale infrastructure or production operations?**

SCADA

7. **Which security control framework uses risk impact levels, data overlays, and/or priority and baseline allocation for control selection?**

NIST SP 800-53

8. **All of these are Asymmetric key algorithms EXCEPT:**

AES

9. **What kind of passive attack focuses on observing how the cryptographic algorithm works?**

Side-channel attack

10. **Each of these components are part of SCADA systems EXCEPT:**

IOT

11. **This type of attack chooses what ciphertext will be decrypted so that the corresponding plaintext can be analyzed?**

Chosen-ciphertext attack

12. **The purpose of information system architecture is PRIMARILY to define:**

How computing components are designed, constructed, and connected

13. **All of these are symmetric key algorithms EXCEPT:**

RSA

3DES

AES

RC

14. **This framework model is focused on developing a risk driven security architecture**

SABSA

15. **AES has 3 different options for creating encryption keys. Which one of these IS NOT an AES key size?**

112 bits

16. **Public Key Cryptography (asymmetric) what kind of keys for encryption and decryption?**

A public and private key

17. **What BEST describes the policies, procedures, safeguards, countermeasures, and other means used to enforce an organizations security needs?**

Security Control

18. **What is a system that is connected by a network in order to share resources and create a single integrated system?**

Distributed system

19. **Before selecting security controls, what is the FIRST thing you should do?**

Know what kind of data needs protection

20. **Which of the following does not apply to a hash algorithm?**

It requires as passphrase or a key

3- Physical Security + Network Security

1. **What type attack is focused on denying availability of information system resources?**

Denial-of-Service

2. **Uninterruptible Power Supplies (UPS) are used to provide what kind of power to the facility?**

Backup power in the form of batteries

3. **All system user accounts must meet all of the following criteria EXCEPT:**

Default passwords must be changed

Have default permissions assigned

Require a strong/complex password

Be uniquely attributed to the user

4. **A DNS poisoning attack:**

Alters a victim's DNS table with incorrect information

5. **What is the TOP priority within physical security?**

Personnel safety and security

6. **Which layer of the OSI model is responsible for converting segments into packets?**

Network Layer

7. **Each of these are Distributed Denial-of-Service (DDOS) attacks, with exception to this one:**

Replay Attack

8. **When creating network access control lists (ACL), how should the ACLs be designed to implement the BEST security?**

Permit traffic by exception

9. **This is NOT a Demilitarized Zone (DMZ):**

A zone that's accessible by the public

10. **What is a facility or room dedicated to housing information system components to support continuous operations?**

Data center

11. **When setting up a Class B network, what is the default subnet mask?**

255.255.0.0

12. **Network Address Translation (NAT) DOES NOT:**

Covert IPv4 addresses into MAC addresses

13. **Which layer of the OSI model is responsible for providing Internet access, sending files, and remote access?**

Application Layer

14. **Which of these is NOT an environmental concerns when it comes to facility location and design?**

Facility lighting

15. **What layer of the OSI model specifies electrical, mechanical, and functional requirements of a network?**

Physical layer

16. **802.1X is a common form of Network Access Controls (NAC) and is frequently paired with what to provide the best security?**

EAP

17. **When an attacker attempts to connect to any wireless network that will permit access, that is called:**

War driving attack

18. **When controlling access to a restricted area, proximity badge readers should be installed and connected to this to provide total security awareness?**

Access Control System

19. **Dedicated environmental controls to a computer room to controlling temperature, static electricity, and humidity is called:**
CRAC
20. **With wireless networks, it's a good security practices to require guest users to access this FIRST:**
Captive portal

4- Virtualization + Access Management + Security Operations

1. **Fuzz testing (fuzzing) is a dynamic test in which testers:**
Push the software to its limits by providing invalid inputs
2. **What is the central program that controls different guest operating systems?**
Hypervisor
3. **What is a drawback to using automated vulnerability assessment tools?**
Scan tools refer to a database of known vulnerabilities
4. **Provisioned hardware, network, storage, and other physical information system infrastructure from a service provider that you do not control is typically referred to as:**
Infrastructure-as-a-Service (IaaS)
5. **A hypervisor is NOT a:**
Cloud based application
6. **A collection of system services and resources made available over the internet is called:**
Cloud Computing
7. **What kind of security assessment evaluates implemented security controls?**
Security Control Assessment
8. **All of these are authentication factors EXCEPT:**
Something you prove
9. **What kind of software assessment test verifies the software and application code construction?**
White box
10. **Operations and maintenance is important to ensure all of the following, EXCEPT:**
The system adds new capabilities to meet organizational needs
11. **What gives a subject direct contact with information system assets**
Access
12. **What component is not considered a technical access control?**
Antivirus software
13. **Virtualization is BEST described as:**
Creating a software-based representation of something rather than a physical one
14. **Using multiple virtualized network resources to create a converged network is referred to as:**
Software Defined Network (SDN)
15. **What access control type reduces authorization (privilege) creep and simplifies enforcing need-to-know and least privilege?**
Role-Based Access Controls
16. **When a username and password is used for identification and authentication, what factor authentication is this?**
Type 1
17. **Each of these are AAA protocols EXCEPT for this one:**
LDAP
18. **The MAIN feature of Discretionary Access Controls (DAC) allows:**
Object owners to control access directly to their objects
19. **This software assessment test analyzes software from user's point of view.**
Black box

20. **A fixed reference point or a set of minimum security controls for a system, network or device describes which term?**

Baseline

5-Incident Response, DRP, and Software Development Security

1+ This type of firewall acts as a go between trusted and untrusted networks, inspecting traffic prior to authorizing a connection:

Proxy Firewall

2+ A stateful firewall performs all of the following EXCEPT:

A. Dynamically allocates a high port number when creating session connection

B. Tracks the state of the connection

C. Uses a state table

D. Clears inactive connections after a set period of time.

3+ An intrusion detection system that detects attacks using a signature or pattern database is called a:

Knowledge based IDS

+4 This backup site is a fully operational replica of the primary operational site

Mirrored Site

5+ Restore the system to normal or functional operations is which phase or step of the incident response process?

Recovery/Remediation

6+ A warm backup site DOES NOT contain this:

Computing devices

7+ If you want to deploy an IDS that detect emerging attacks better than any other option, what should you choose?

Behavior-Based IDS

8+ A violation of a security policy is called what?

Security incident

9+ What is a computing device that is intentionally configured with known vulnerabilities aimed at attracting attackers?

Honeypot

10+ Copying and transmitting digital information to an offsite storage location is known as:

Electronic Vaulting

11+ A worm is a:

Self-replicating and self-contained application that executes malicious code

12+ You've been seeing a lot of activity on the network and find yourself responding to too many alerts to adequately respond to. You would like the system to actively respond to potential system attacks to ensure these attacks are stopped before they occur.

Network IPS

13+ To properly maintain a firewall, which of these is LEAST important?

Monitor operational end-of-support/end-of-life of the firewall

14+ What type of attack uses digital communication messages to collect private or sensitive information?

Phishing

15+ The first phase of incident response is to identify if an event has occurred?

Detection

16+ What focuses on preventing unnecessary security risks in developed software?

Secure coding

17+ A firewall server, that has a minimal attack surface, placed between an internal and external network, is called:

A bastion host

18+ Cross-Site Request Forgery (CSRF) attacks focus on:

Tricking a user to perform unwanted actions on a web application

19+ Creating a situation where a victim feels required to help an attacker is also known as:

Quid pro quo attacks

20+ The use of a telephone based system to carry out a phishing attack is called:

Vishing

Knowledge Check: CISSP Crash Course Final Exam

- 1. Due care can be explained as:**
The reasonable effort to protect an asset
- 2. Each of these components are part of SCADA systems EXCEPT:**
IOT
- 3. A hypervisor is NOT a:**
Cloud based application
- 4. What focuses on preventing unnecessary security risks in developed software?**
Secure coding
- 5. This type of firewall acts as a go between trusted and untrusted networks, inspecting traffic prior to authorizing a connection:**
Proxy Firewall
- 6. What type of security control is used to address a known risk, vulnerability, or threat that cannot be mitigated directly**
Compensating control
- 7. An example of a security standard is:**
The requirements to securely configure a software application
- 8. Fuzz testing (fuzzing) is a dynamic test in which testers:**
Push the software to its limits by providing invalid inputs

9. A worm is a:
Self-replicating and self-contained application that executes malicious code
10. When an organization wants to declare very detailed and short-range security goals and objectives, this should be documented in a:
Operational Plan
11. When setting up a Class B network, what is the default subnet mask?
255.255.0.0
12. Uninterruptible Power Supplies (UPS) are used to provide what kind of power to the facility?
Backup power in the form of batteries
13. The first phase of incident response is to identify if an event has occurred?
Detection
14. Using multiple virtualized network resources to create a converged network is referred to as:
Software Defined Network (SDN)
15. What is a computing device that is intentionally configured with known vulnerabilities aimed at attracting attackers?
Honeypot
16. When determining the value of an organizational asset, which is LEAST important
How long it will take to replace the asset
17. What kind of software assessment test verifies the software and application code construction?

White box

18. Which of the following does not apply to a hash algorithm?
It requires a passphrase or a key
19. What gives a subject direct contact with information system assets
Access
20. Cross-Site Request Forgery (CSRF) attacks focus on:
Tricking a user to perform unwanted actions on a web application
21. What kind of security assessment evaluates implemented security controls?
Security Control Assessment
22. A warm backup site DOES NOT contain this:
Computing devices
23. Which of these is NOT an environmental concern when it comes to facility location and design?
Facility lighting
24. Operations and maintenance is important to ensure all of the following, EXCEPT:
The system adds new capabilities to meet organizational needs
25. What component is not considered a technical access control?
Antivirus software
26. Virtualization is BEST described as:
Creating a software-based representation of something rather than a physical one
27. Data is MOST vulnerable when it is:
In transit
28. If you cannot determine how much a system asset costs, what is the best approach to perform a risk assessment?
A qualitative risk assessment
29. All of these are authentication factors EXCEPT:
Something you prove
30. A fixed reference point or a set of minimum security controls for a system, network or device describes which term?
Baseline
31. What kind of passive attack focuses on observing how the cryptographic algorithm works?
Side-channel attack

32. What is a drawback to using automated vulnerability assessment tools?
Scan tools refer to a database of known vulnerabilities
33. What is NOT a common technique to implement confidentiality in an information system?
Hashing
34. The 3 main categories of security controls are:
Administrative, physical, and technical
35. What is a facility or room dedicated to housing information system components to support continuous operations?
Data center
36. When performing a cost/benefit analysis, which is NOT a consideration when making a risk based decision?
Determining how much information to provide senior management so that they can make a decision
37. What access control type reduces authorization (privilege) creep and simplifies enforcing need-to-know and least privilege?
Role-Based Access Controls
38. A stateful firewall performs all of the following EXCEPT:
Dynamically allocates a high port number when creating a session connection
39. When using SHA to hash an input value, what key size would create the STRONGEST encryption?
512 bits
40. Which one of the following is NOT a canon of the COE?

Always provide the best possible security protection based on your current knowledge and skill level

41. Each of these are AAA protocols EXCEPT for this one:
LDAP
42. To discover the potential loss for a single security occurrence, the proper formula to use is:
 $AV * EF$
43. 802.1X is a common form of Network Access Controls (NAC) and is frequently paired with what to provide the best security?
EAP
44. The purpose of information system architecture is PRIMARILY to define:
How computing components are designed, constructed, and connected
45. The states of data are comprised of each of these but DOES NOT include this:
Data in process
46. Michael is a new security engineer working for a small company. He received notification from a firewall vendor stating the operating system had a critical vulnerability and a patch update was available to correct the vulnerability.
Follow the established security policy for handling patch updates
47. When a username and password is used for identification and authentication, what factor authentication is this?
Type 1
48. AES has 3 different options for creating encryption keys. Which one of these IS NOT an AES key size?
112 bits
49. DevOps is the process of combining system development and operations into a continuous process. When assessing the security architecture, what is one of the most important parts of DevOps security?
Security must be integrated into DevOps as part of system and security architecture
50. An intrusion detection system that detects attacks using a signature or pattern database is called a:
Knowledge based IDS

