THE EFFECTIVE CISSP®

PRACTICE QUESTIONS

First Edition

Wentz Wu

THE EFFECTIVE CISSP®

PRACTICE QUESTIONS

First Edition

Wentz Wu

THE EFFECTIVE CISSP PRACTICE QUESTIONS

First Edition

Wentz Wu

The Effective CISSP
Practice Questions

Published by Wentz Wu (https://WentzWu.com)

Cover Designer: CHING I.HSU

To all those who learn and wave the sword of security to protect our cyberspace and society.

ACKNOWLEDGMENTS

Writing a book is as challenging as taking the CISSP exam. It takes time to develop good results. I am grateful that my friends, Aaron, Daniel, Pato, Steve, and Tac, have been supportive and accompanying me on my journey. More than words can say my gratitude.

I would like to convey my sincerest thanks to my Effective CISSP group members, blog readers, and CISSP students in Taiwan. Your active engagement, responses, comments, and feedback make this book possible.

Special thanks go to our fellow CISSP, Fadi Sodah, and Sven De Preter, for reviewing this book. They are also the reviewers of my first book, The Effective CISSP: Security and Risk Management.

Thanks to the following groups and communities for inspiring me and advancing the profession:

- CISSP Exam Preparation - Study Notes and Theory
- CISSP, CISM and PMP certification training by Thor Teaches!
- Information Audit
- Get CISSP Certified
- Certification Station on Discord

This book would not have been possible without your support and assistance.

Warmest regards,
Wentz Wu

PREFACE

This book, aka **CISSP Sudoku 365** , is a compilation of Wentz QOTD questions for the past year. They are available on my blog (https://WentzWu.com) for free if used for non-profit purposes.

I publish this book as the anniversary milestone of my persistent authoring. I hope this harmonized version can serve as the manual or blueprint of Wentz QOTD for CISSP aspirants. This book provides excellent navigation experience between questions, answers, and explanations.

Practicing questions is an exchange of perspectives and learning process. I design questions, suggest the answer, and justify and explain answers based on my experience and knowledge. However, the answer key or so-called correct answer to each question is subject to its context and the reader's knowledge and perspective. So, you will always see "my suggested answer." Your reasoning process and justification are more valuable than answering the question right.

This book contributes to your success in the CISSP exam, but it's not sufficient. You need more "quality" questions. Not all questions are created equal. If you have tried Wentz QOTD and not retreated, you may feel more comfortable in the real exam.

I hope you pass the CISSP exam as soon as you have planned!

ABOUT THE AUTHOR

Wentz Wu is the co-founder of Amicliens and has been working in the IT industry for more than 20 years. He is devoted to applying information technologies to solve business problems, delivering training and education courses, and giving back to the community.

In his professional career, Wentz is skilled at implementing IT infrastructure and cloud services, developing quality software, conducting comprehensive business analysis, managing projects with agility, and advising and delivering practical business solutions.

With a solid technical background and business savvy, Wentz comprehensively offers the CISSP course based on the Amicliens InfoSec Conceptual Model, which effectively addresses the official (ISC)² CISSP exam outline.

As a lifelong learner, Wentz demonstrates his endeavor and achievement as follows:
- EMBA/CBAP/PMP/ACP/PBA/RMP
- CGEIT/CISM/CRISC/CISA
- CISSP-ISSMP,ISSEP,ISSAP/CCSP/CSSLP
- CEH/ECSA/AWS-CSAA/MCSD/MCSE/MCDBA
- SCRUM: PSM Level I/PSPO Level I/PSD Level I
- ISO 27001 LA/ISO 27701 LA Courses Completed

Wentz can be reached through:
Email: wentzwu@gmail.com
Blog: https://WentzWu.com
Facebook: https://www.facebook.com/groups/EffectiveCISSP
YouTube: https://www.youtube.com/c/EffectiveCISSP

TABLE OF CONTENTS

GET STARTED

CISSP Sudoku 365!

This book has a nickname, **CISSP Sudoku 365** , a metaphor of turning the 365 questions into the exciting game, Sudoku. It is a selection of Wentz's Question of The Day for CISSP, aka **Wentz QOTD** , an initiative for giving back to the community. As a CISSP instructor in Taiwan, Wentz spends two hours on average each day to author the question and develop the solution.

For more CISSP practice questions and resources, please visit:

- https://WentzWu.com/QOTD
- https://WentzWu.com/CISSP

The Audience of This Book

This book is for CISSP aspirants who:

1. intend to learn by topics,
2. finish the first round of study, or
3. sprint for the CISSP exam.

Reasoning and Justification

This book not only provides guidance to those questions but also advocates **reasoning** and **justification** . Most of the questions synthesize two or more facts and entail an analysis of the implications. To use this book effectively, CISSP aspirants need to:

1. think, research, and study intensively,
2. use judgment and critical thinking, and
3. develop justification and identify the best answer.

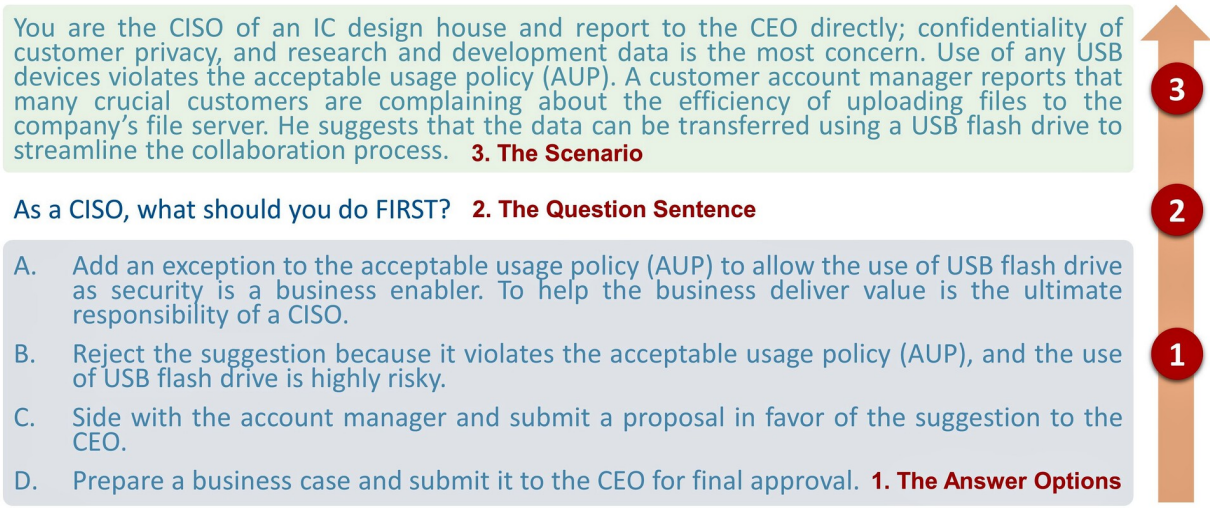
Kindly be reminded that the suggested answer is for your reference only. It doesn't matter whether you have the right or wrong answer. What really matters is your reasoning process and justifications.

Exam Answering Skills

There are three basic skills: reverse reading, identifying sequence, and, and eliminating aliens.

☐ Reverse reading

Browse the question in the **reverse order** to grasp the **main idea** of the question and to catch the **intuitive answer** at the first impression. Intuition triggers your powerful deep mind.



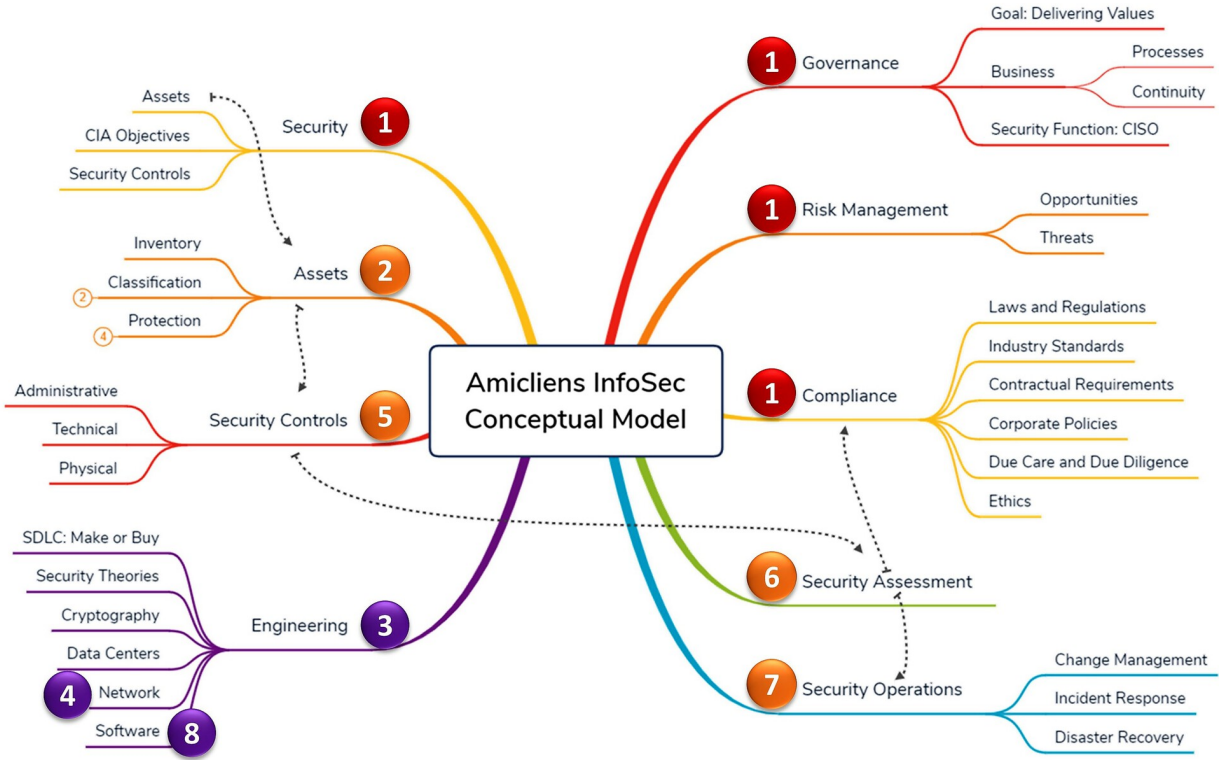
☐ Identifying Sequence

Answer options may be **s equential** but arranged in random order. Being aware of this arrangement and identifying the correct sequence helps answer the questions with "FIRST" or "MOST."

☐ Eliminating Aliens

Eliminating aliens means ruling out those options that are apparently wrong. Select the survivor as your answer; don't rely on selecting the so-called "correct answer."

A Reference CISSP Conceptual Model



Handy Navigation Experience

1. **Which of the following statement best describes confidentiality?**

A. How the system protects data from unauthorized access
B. Access to the system by authorized personnel
C. How the system prevents the disclosure of information
D. Process of determining the identity of a user

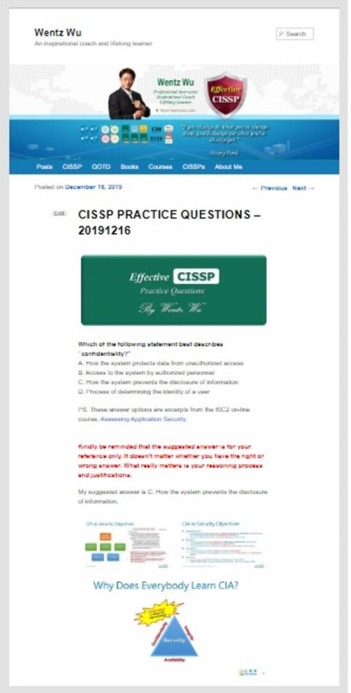
☞ Answer to QOTD: 20191216

2. To Wentz QOTD for detail explanation

1. Back and forth the Question and Answer

ANSWER KEYS

1	20191216	C. How the system prevents the disclosure of information.



DOMAIN 1: SECURITY AND RISK MANAGEMENT

CIA AS SECURITY OBJECTIVES

1. **Which of the following statement best describes confidentiality?**

   A. How the system protects data from unauthorized access
   B. Access to the system by authorized personnel
   C. How the system prevents the disclosure of information
   D. Process of determining the identity of a user

   ☞ Answer to QOTD: 20191216

2. **When talking about the sensitivity of the information, which of the following is least related?**

   A. Confidentiality
   B. Integrity
   C. Non-repudiation
   D. Availability

   ☞ Answer to QOTD: 20200526

3. **Which of the following information security properties or objectives is not defined in the Federal Information Security Management Act (FISMA) of 2002?**

   A. Non-repudiation
   B. Accountability
   C. Authenticity
   D. Availability

   ☞ Answer to QOTD: 20200101

4. **Alice sent an email to Bob with a legally-binding digital signature.**

Which of the following best describes the security objective Alice wants to achieve?

A. Confidentiality
B. Integrity
C. Availability
D. Accounting

☞ Answer to QOTD: 20200410

5. **Information Security is a discipline to protect assets from threats through safeguards to achieve the objectives of confidentiality, integrity, and availability, or CIA for short, support business processes, and create and deliver values.**

   All of the following hinder or enforce the security objective of integrity, except which one?

   A. A recipient denied having received a message
   B. A disgruntled employee deleted confidential files
   C. A middle man poisoned a DNS
   D. A sender signed an email with digital signature

   ☞ Answer to QOTD: 20191201

SECURITY GOVERNANCE

6. **As a CISO, which of the following should you develop first?**

   A. Information security policies
   B. Business continuity program
   C. Information security strategy
   D. Incident response capacity

   ☞ Answer to QOTD: 20200417

7. **You are the new CISO of an international trading company and just got on board recently.**

   Which of the following is the first and most concern for you?

   A. Salary and benefits package
   B. The role and responsibility (R&R) of CISO
   C. To develop and implement an information security strategy
   D. To elicit business and security requirements, and develop an information security program and supporting policies

   ☞ Answer to QOTD: 20190501

8. **You are the newly recruited CISO for a global company. After studying the mission vision, strategic goals, corporate strategy, and business and security requirements, you start to develop the information security strategy.**

   Which of the following should you conduct first?

   A. Determine the blueprint and milestones
   B. Conduct gap analysis

C. Consider resources and constraints
D. Develop an information security program policy

☞ Answer to QOTD: 20190922

9. **You are a newly recruited CISO working for a direct bank based in Taiwan that relies entirely on internet banking.**

   Which of the following should you do first?

   A. Meet and talk to stakeholders
   B. Initiate an information security program
   C. Conduct a thorough risk assessment
   D. Formulate a cybersecurity strategy

   ☞ Answer to QOTD: 20200102

10. **Which of the following best describes the idea of the strategic alignment of the security function?**

    A. Create a dedicated position of CISO and delegate the CISO in charge of information security.
    B. Wake up the awareness of the CEO and the board of directors that they are liable for including information security into the agenda of corporate strategy
    C. Mitigate risks to the acceptable level of senior management to achieve confidentiality, integrity, and availability.
    D. Govern or manage information security with a business mindset to deliver values.

    ☞ Answer to QOTD: 20190908

11. **You are the CISO of an IC design house and report to the CEO directly; confidentiality of customer privacy, and research and development data is the most**

concern. The use of any USB devices violates the acceptable usage policy (AUP).

A customer account manager reports that many crucial customers are complaining about the efficiency of uploading files to the company's file server. He suggests that the data can be transferred using a USB flash drive to streamline the collaboration process.

As a CISO, what should you do FIRST?

A. Add an exception to the acceptable usage policy (AUP) to allow the use of USB flash drive as security is a business enabler. To help the business deliver value is the ultimate responsibility of a CISO.
B. Reject the suggestion because it violates the acceptable usage policy (AUP), and the use of USB flash drive is highly risky.
C. Side with the account manager and submit a proposal in favor of the suggestion to the CEO.
D. Prepare a business case and submit it to the CEO for final approval.

☞ Answer to QOTD: 20190423

12. **You are recruited to fill the newly created position of CISO, which was unofficially assumed by the CIO to govern the information security affairs. You are hired to report to the CEO directly, as the peer officer with CIO, and responsible for formulating and executing information security strategies.**

Which of the following best justifies this arrangement?

A. Separation of duties
B. Avoidance of Conflict of Interest
C. Strategic and business alignment
B. Legal or regulatory requirements

☞ Answer to QOTD: 20190916

13. **You are the CISO of a global company and participating in an executive meeting with an agenda to acquire a company as part of the corporate growth strategy. The CEO is concerned with the compliance of due diligence in this acquisition.**

    As a CISO, which of the following is the best for you to contribute to this project?

    A. Review the acquisition contract and identify potential contractual risks
    B. Build a tiger team to conduct security testing to identify potential vulnerabilities and threats.
    C. Train and educate the security staff of the acquired company about corporate security policies.
    D. Conduct a comprehensive security assessment and identify the gap between corporate security policies.

    ☞ Answer to QOTD: 20190915

14. **Your company plans to create a new position, CISO. It is responsible for formulating and executing information security strategies.**

    The board of directors is holding a meeting to revise the Corporate bylaws and calls for the conclusion that the CISO shall report to the audit committee.

    As the CEO attending the meeting, which of the following is the best feedback?

    A. Agree with the resolution as it's a good arrangement.
    B. Suggest that internal audit capability should be put in the job skills of CISO.
    C. Propose a clause to separate the CISO and CIO role to avoid conflict of interests.

D. Remind that the independence of auditing would be hindered.

☞ Answer to QOTD: 20190917

15. **Your company, as a Taiwan-based public company, decides to start the business of selling toys online and shipping globally. To penetrate the market in the US, your company set up a branch company in the United States. The governance model is centralized; only the decisions that must be compliant with local laws and regulations are delegated to the local branch. The local data retention policy of the US branch is different from the local laws and regulations. As a security professional for the local branch, which of the following is the best action?**

A. Review the local data retention policy
B. Suggest the local branch follow the policy of headquarters
C. Request corrective actions to be compliant with the local laws and regulations
D. Revise the local policy to meet the requirements of the local laws and regulations

☞ Answer to QOTD: 20191017

16. **Your company decides to start the business of selling toys online and shipping globally as a strategic move. You are going to be designated as the program manager for the E-commerce program that is sponsored by the COO and tasks an in-house development team to develop the E-commerce system to support the new business. Which of the following is most critical to your success?**

A. Competent team
B. Communicated Policy

C. Executable strategy
D. Documented program plan

☞ Answer to QOTD: 20191224

17. **You are the CISO working for a direct bank based in Taiwan that relies entirely on internet banking. You are developing the information security policy to build a policy framework for related supporting policies, and considering its objectives, scope, and roles and responsibilities.**

Which of the following is the best to be enlisted in the policy scope?

A. Levels of data sensitivity
B. Senior management
C. Stakeholders covered by the policy
D. Confidentiality, integrity, and availability

☞ Answer to QOTD: 20200112

18. **The board of directors is not happy with the effectiveness and performance of IT investments in your organization. As a security professional, you are engaging in the improvement initiative to address both business and security requirements in IT investments.**

Which of the following is the most effective management practice?

A. Conducting cost/benefit analysis
B. Establishing enterprise architecture
C. Developing a comprehensive information security policy
D. Evaluating the trustworthiness of ICT services, products, and suppliers

☞ Answer to QOTD: 20200205

19. **As a CISO, you report to the CEO directly and are invited, from time to time, to sit in the board room for consulting.**

Which of the following best assures the CEO, the board, and other stakeholders that information security governance is sound and appropriate?

A. Information security policy
B. Security audit
C. Risk assessment
D. Information security strategy

☞ Answer to QOTD: 20200518

RISK MANAGEMENT

21. **According to ISO 31000, the risk is the "effect of uncertainty on objectives." Which of the following is a risk?**

    A. The mother nature
    B. Sabotage
    C. The loss of 5 million of monetary value
    D. None of the above

    ☞ Answer to QOTD: 20200527

22. **Before an organization is attempting to conduct risk analysis, what should they identify first?**

    A. Threat sources and threat events
    B. Exploitable weaknesses/deficiencies
    C. Impacts or consequences of concern and critical assets
    D. Any of the above can go first

    ☞ Answer to QOTD: 20191015

23. **As a CISO, you decide to implement Information security management systems and to be certified as compliant with ISO 27001 standard, in which actions to address risks and opportunities are required. You realize this requirement is about risk management and start evaluating risk management frameworks to meet the requirement.**

    To implement a risk management program, which of the following least meets the requirement?

    A. NIST FARM Framework (Frame, Assess, Respond, and Monitor)
    B. ISO 27002

C. ISO 27005
D. ISO 31000

☞ Answer to QOTD: 20191018

24. **Your company decides to start the business of selling toys online and shipping globally. The E-Commerce system that supports the new business will be developed in-house. In a threat modeling meeting, the project team is analyzing and prioritizing the risks.**

As a security professional, which of the following is the best to prioritize risks?

A. Annual Rate of Occurrence (ARO)
B. Risk exposure
C. Business Impact Analysis (BIA)
D. Estimated financial loss

☞ Answer to QOTD: 20191021

25. **Your company decides to start the business of selling toys online and shipping globally. The E-Commerce system that supports the new business will be developed in-house. The project team identified some risks as follows:**

R001 - The company's reputation might be damaged.
R022 - The business process of shipping might be disrupted.
R003 - The attackers might initiate distributed denial of services (DDOS).

Aa a security professional, which of the following should be mitigated first?

A. R001
B. R002

C. R003
D. None of the above

☞ Answer to QOTD: 20191028

26. **You are the CISO working for a direct bank based in Taiwan that relies entirely on internet banking. You are concerned that the hacker can type in SQL expressions in the login form to bypass the authentication.**

Which of the following best describes your concern?

A. Risk exposure
B. Threat event
C. Threat scenario
D. Risk profile

☞ Answer to QOTD: 20200103

27. **You are the CISO working for a direct bank based in Taiwan that relies entirely on internet banking. You are evaluating security control frameworks to mitigate risks and enforce security.**

Which of the following is least likely to be included in a security control framework?

A. Residual risk after implementing controls
B. Audit procedure or assessment methods
C. The process to eliminate controls from baselines
D. Implementation guidance for access control

☞ Answer to QOTD: 20200113

28. **You are the CISO working for a direct bank based in Taiwan that relies entirely on internet banking. Your bank is considering outsourcing the customer**

relationship management (CRM) system to an offshore software development vendor.

Which of the following action should your bank take first?

A. Conduct the threat scenario analysis
B. Describe threat sources that are relevant to the organization
C. Develop and select threat events for analysis
D. Determine applicable controls

☞ Answer to QOTD: 20200120

29. **Your organization adopts the NIST FARM risk management approach to frame, assess, respond to, and monitor risks that arise from a variety of sources or tiers such as information systems, business processes, or the organization. As a CISO, you are considering the governance structures from the organizational perspective to address risk.**

    Which of the following is not your primary concern?

    A. Strategies for internal development and external acquisition of IT products
    B. Risk management strategy
    C. Approaches to replacing legacy information systems
    D. Enterprise Architecture

    ☞ Answer to QOTD: 20200127

30. **You are the manger authorized to make decisions on the acceptance of risk. After risk treatment, you are considering a case that the cost of handling the residual risk is much higher than the risk acceptance criteria. Even though quantitative economic benefits cannot justify it, you deeply believe the risk with low likelihood is not urgent but brings a significant impact**

on the organization and should be handled. Which of the following decisions best meets the risk acceptance principles?

A. No further treatment because it doesn't meet the risk acceptance criteria
B. No further treatment because subjective judgment is not reliable
C. Revise the risk acceptance criteria if possible, and implement risk treatment
D. Implement exception risk treatment but comment and justify your decision.

☞ Answer to QOTD: 20200129

31. **Your company decides to invest in solutions, in the coming year, to support salespeople as road warriors and boost sales. Laptops, mobile phones, VPN, wireless networks, and customer relationship management (CRM) systems are parts of the selected solution. As a CISO, which of the following is the least concern when developing a risk management strategy?**

A. Foreign ownership, control, or influence over suppliers
B. Investment strategies
C. The impact of the solution upon business processes
D. Laws and regulations

☞ Answer to QOTD: 20200201

32. **Your company is considering solutions to boost sales. The head of the sales department suggests implementing the CRM system and provisioning salespeople with mobile devices and VPN connections. The IT manager points out that this solution may lead to personal data leakage and cause**

substantial financial loss. As a security professional, you are assessing this risk.

Which of the following approach is most effective?

A. Use qualitative analysis to determine the likelihood and impact of the risk
B. Conduct quantitative analysis to determine the possibility and monetary loss of the risk
C. Determine the risk exposure and identify risk tolerance
D. Conduct business impact analysis (BIA) to determine the organization-wide impact

☞ Answer to QOTD: 20200203

33. **Your company is considering purchasing new tablets to support salespeople and boost sales. As a senior procurement manager, you are framing the risk context of the information and communications technology supply chain risk management (ICT SCRM).**

Which of the following should you consider first?

A. Mission functions
B. Types of suppliers (COTS, external service providers, or custom, etc.)
C. Strategic supplier relationships
D. Technologies used organization-wide

☞ Answer to QOTD: 20200204

34. **Organizations are facing different types of risks that hinder the pursuit of organizational objectives. As a security professional, you are a member of the risk management program. Which of the following is the least likely to conduct when establishing the risk context?**

A. Determine risk tolerance
B. Provide a reference risk model
C. Build enterprise architecture
D. Assign a risk executive

☞ Answer to QOTD: 20200207

35. **You've learned about from a CISSP study guide the formula, total risk = threats × vulnerability × asset value, and used it in your risk management program. You identified that hacktivists and script kiddies might employ SQLMap to initiate SQL injection to attack database systems through the web servers. The asset value of customer profiles classified as CONFIDENTIAL is worthy of 5 million US dollars. They are processed on the web-based CRM system that is very vulnerable because of poor design and delayed patches.**

    You are conducting a risk assessment, which of the following is the least common and cost-ineffective expression of the total risk?

    A. USD$7,438,399.5
    B. LOW
    C. 25
    D. VERY HIGH

    ☞ Answer to QOTD: 20200217

36. **Because of being subject to the risk of data integrity and availability, some global cloud service providers give up building data centers in regions where power supply is unstable.**

    Which of the following risk treatment options or risk response strategies best describes the decision?

A. Risk elimination
B. Risk rejection
C. Risk aversion
D. Risk avoidance

☞ Answer to QOTD: 20200306

37. **An information system has been authorized to operate. Which of the following is the least concern when monitoring risk at the information system level?**

A. Compliance
B. Residual risk
C. Emerging changes
D. Ongoing authorization

☞ Answer to QOTD: 20200419

38. **Your company is a well-known cloud services provider. You learned about from a threat intelligence report that the Meltdown and Spectre bugs are hardware-level vulnerabilities affecting almost all brands of CPUs.**

The Meltdown attack allows a rogue process exploiting the race condition to read all memory space and leads to unauthorized access.

The Spectre attack is a timing attack employing the speculative execution so that even a scripted malware can read all the process's memory.

After iterations of risk treatments, the latest software patches still hinder the system performance significantly. Supported by considering all the risk treatment options, the senior management decides to accept the risk.

Which of the following least reflects the management decision?

A. Monitor and respond to the risk until the risk materializes
B. The risk exposure of inherent risk is lower than the risk acceptance criteria
C. The risk exposure of residual risk is lower than the risk acceptance criteria
D. Leave the risk in the risk register and keep monitoring it

☞ Answer to QOTD: 20200501

COMPLIANCE

39. **You are sitting for the CISSP exam. An agreement is displayed on the screen requiring that you, as an exam taker, cannot share any content of the exam with others. After reviewing it, you click "I agree" and proceed to start the exam.**

    Which of the following best describes your behavior?

    A. Accountability
    B. Digital signature
    C. Due care
    D. Due diligence

    ☞ Answer to QOTD: 20191220

40. **You are preparing for the CISSP exam. There are vendors spreading advertisements claiming the offer of real exam dumps or the opportunity to get certificates without testing.**

    As a CISSP aspirant, which of the following (ISC)² Code of Ethics Canons is violated and specified in a complaint ? Why**?**

    A. Act honorably, honestly, justly, responsibly, and legally
    B. Provide diligent and competent service to principals
    C. Advance and protect the profession
    D. None of the above

    ☞ Answer to QOTD: 20200108

41. **Your company decides to start the business of selling toys online and shipping globally. A newly recruited developer, Jack, is hired because of a critical algorithm published in his graduate thesis.**

He joined the in-house development team and developed a software component for shopping cart analysis from scratch that copied the idea from his previous company, which claims to have the patent of the algorithm.

As a security professional, which of the following is the most concern?

A. Trademark
B. Trade secret
C. Patent
D. Copyright

☞ Answer to QOTD: 20191222

42. **Your company is a direct bank that relies entirely on internet banking; its shares are public-traded. You are exercising due diligence surveying applicable laws and regulations to your company.**

    Which of the following has a profound effect on corporate governance and holds directors and officers personally liable for the accuracy of financial statements?

    A. GDPR
    B. GLBA
    C. SOX
    D. HITECH

    ☞ Answer to QOTD: 20200222

43. **You are the CISO working for a direct bank based in Taiwan that relies entirely on internet banking. You are reviewing applicable legal and regulatory requirements for compliance.**

    Which of the following will concern you most?

A. Procurement staff issued a contract without minimum security requirements
B. The development team used an open-source component with an unknown source
C. Policies are published after a new law or regulation as a reactive response
D. Personal data is open for the data subject to update

☞ Answer to QOTD: 20200117

PERSONAL DATA AND PRIVACY

44. **Your company is selling toys online and ship globally. To study the preference of consumers, the marketing department designed an anonymous survey and put it onto the official web site for visitors to fill out. However, the head of the marketing department demands that the survey collect the city of the visitor for regional analysis.**

    Taking account of the privacy issue, which of the following privacy principles should be followed?

    A. Reasonable expectation of privacy
    B. Defense in depth
    C. Consent and choice
    D. None of the above

    ☞ Answer to QOTD: 20190926

45. **Your company decides to sell toys online and ships globally. The in-house team and an outsourced team are collaborating to develop the online shopping website. The outsourced team is requesting customer data for software testing. The customer data are hashed, then masked with a star (*) symbol to prevent disclosing information about the subject to protect privacy. Which of the following best describes the de-identification technique?**

    A. Anonymization
    B. Scrambling
    C. Deprivacy digesting
    D. Pseudonymization

    ☞ Answer to QOTD: 20200317

46. **An employee's sharing pictures taken in the office or daily life is subject to data disclosure. Which of the following security control is the most effective and should be implemented first to ensure security?**

A. Data Loss Prevention (DLP) solutions
B. Bring Your Own Device (BYOD) solutions
C. Acceptable use policy (AUP)
D. Security awareness training

☞ Answer to QOTD: 20200416

47. **Your company is engineering an information system to support the new business of selling toys online in the United States.**

The marketing department proposed that the system shall retrieve the customer profile from social media when the customer is signing up to ease and accelerate the registration process. They decide to accept domestic orders only and reject orders from EU citizens to avoid legal and regulatory risks.

As a security professional, you are aware that the privacy issue should be addressed.

Which of the following will most concern you?

A. Principal's Consent
B. Use, retention and disclosure limitation
C. Legal and regulatory requirements
D. Accountability

☞ Answer to QOTD: 20190911

PERSONNEL SECURITY

48. **Mandatory vacation and job rotation are implemented in your company to detect and prevent corruption. As a security professional, which of the following will you suggest with priority?**

A. Conduct user entitlement review periodically
B. Isolate employees from enterprise networks when an audit is undergoing on their mandatory vacation
C. Provide training and certification courses upon rotation to ensure the new job can be done effectively
D. Require immediate password change when an employee rotates to a new position

☞ Answer to QOTD: 20191124

49. **You are working for an IC design house. Confidentiality of customer privacy and research and development data is the most concern. Jack, as a disgruntled security administrator, received a new job offer from a company and notified the human resources department of resignation one week before. The HR staff considers it is an unfriendly leave.**

As a security professional, which of the following will you least likely suggest?

A. Terminate his access to systems immediately
B. Assign him to a restricted area during the notice of resignation
C. Require him to prepare handover documentation
D. Remove him from the offices and ask him to stay home

☞ Answer to QOTD: 20191130

50. **As a CISO working for a direct bank based in Taiwan that relies entirely on internet banking, you are**

collaborating with the Human Resources (HR) department to improve personnel security.

Which of the following will you suggest to review first?

A. Role-based access control mechanisms
B. Background investigation procedures
C. Implementation of separation of duties
D. Effectiveness and correctness of job descriptions

☞ Answer to QOTD: 20200122

51. **You are the instructor conducting the security awareness training of your company. You are giving examples of social engineering attacks, which of the following is the best example of a user's behavior that might lead to a threat scenario that the threat source has the lowest costs to collect information about system configurations?**

A. Post job positions on online job portals
B. Share photos on social media
C. Explore an unknown USB dongle on computers
D. Share emails with colleagues

☞ Answer to QOTD: 20200609

DOMAIN 2: ASSET SECURITY

ROLES AND RESPONSIBILITIES

52. **You are planning the program for security awareness, training, and education. Which of the following is not the primary target audience who needs more knowledge and skills that will enable them to perform their jobs more effectively?**

    A. All employees
    B. End-users
    C. Security administrators
    D. IT engineers

    ☞ Answer to QOTD: 20200628

53. **Your company finished conducting an asset inventory. As the head of the sales department, you are assigned as the data owner of the customer master data. You are learning about the role and responsibility of the data owner.**

    Which of the following is least related to the data owner?

    A. Classify the data based on business value
    B. Delegate the system administrator to authorize users
    C. Take the ultimate responsibility if the data is breached
    D. Define the classification scheme

    ☞ Answer to QOTD: 20190923

54. **Your company finished conducting an asset inventory. As the head of the sales department, Sandy is assigned as the data owner of the customer master data.**

The sales processes are supported by the ERP system, which is tasked to process data from different departments and is owned by the CIO, Cynthia – the system owner.

In a meeting of the information security steering committee, Sandy proposes that multi-factor authentication should be implemented on the ERP system to ensure sufficient security level to protect the customer master data.

As a chairperson, how should the proposal be addressed?

A. Implement the multi-factor authentication as Sandy is the data owner of the customer master data
B. Ask Sandy to provide suggested multi-factor authentication solutions
C. Have Cynthia in charge of the proposal
D. Call for votes on the spot to determine if the proposal is accepted

☞ Answer to QOTD: 20190924

55. **Your company is retiring 50 personal computers and 50 laptops, which have been depreciated for five years with inconsiderable accounting residual values.**

Employees are eligible to buy those retired devices for personal or home use with first priority. The remaining devices will be sold in public. Full disk encryption is enabled on all the laptops to ensure the security of mobility.

To best address the issue of data remanence, which of the following should be conducted?

A. Use the operating system companion utility to format all the disks fully

B. Use the "reset to factory default" function to remove all the data on personal computers and laptops
C. Use the vendor-provided utility with the dedicated commands to purge all the data
D. Crypto-erase the disks on the laptops and degauss the magnetic disks on the personal computers

☞ Answer to QOTD: 20190925

56. **Your company is selling toys online and ship globally. The business is supported by an E-Commerce system developed in-house and deployed to a public cloud with the Platform as a Service (PaaS).**

Your company collects customer data for the purpose of billing and shipping. As a security professional, you are identifying the role of your company and applicable laws and regulations in terms of privacy.

Which of the following best describes the role of your company?

A. Data Owner
B. Data Custodian
C. Data Controller
D. Personally Identifiable Information (PII) Principal

☞ Answer to QOTD: 20190927

57. **Information is the asset of the organization. Which of the following refers to the careful and responsible management of information belonging to the organization as a whole, regardless of the entity or source that may have originated, created, or compiled the information?**

A. Information custodianship
B. Information assurance

C. Information stewardship
D. Information ownership

☞ Answer to QOTD: 20200208

58. **Your organization is developing a Transportation Management System (TMS) that processes two types of data: air and ground transportation data. It is about time to categorize the system to determine baseline security controls.**

Which of the following roles least participates in the system categorization process?

A. Executive management
B. Data custodian
C. Information owner
D. System owner

☞ Answer to QOTD: 20200212

59. **Asset ownership is one of the primary issues in information security. After taking inventory of the information asset, your organization is reviewing the ownership.**

Which of the following has the least ownership controversy?

A. Commercial-Off-The-Shelf (COTS) software
B. Original equipment manufacturer's (OEM) production parameters or formula
C. Customer profile
D. Inventions of research and development

☞ Answer to QOTD: 20200214

60. **Your company sells toys online worldwide. A web-based E-Commerce system developed in-house**

supports the business. The EC system, owned by the IT manager, processes a variety of data owned by department heads. As a CISO, which of the following is the best arrangement to determine security controls for the EC system?

A. You
B. Data owners
C. The System owner
D. The IT manager and data owners

☞ Answer to QOTD: 20200613

61. **An offboarding sales representative downloaded customer profiles owned by the head of the sales department from the file server onto a USB dongle on the day he left and sold it online. This data breach occurred because of the miscommunication between the HR and IT departments. The HR department didn't notify the IT department to disable the user accounts and revoke the privileges of the unhappy employee in time.**

As a CEO, which of the following roles do you think is accountable for the data breach of customer profiles?

A. The system owner of the file server, due to inappropriate security controls
B. The vice president of HR, owing to lack of due care
C. The CIO, because of ineffective IT support for user provisioning/deprovisioning
D. The vice president of Sales, for the responsibility and authority of classification and protection

☞ Answer to QOTD: 20200707

ASSET CLASSIFICATION

62. **You have been just officially endorsed as a CISSP and got promoted as the CISO. To meet legal and regulatory requirements, you issued a policy to direct and sponsor the data governance program.**

    Which of the following should be conducted first?

    A. Classify data
    B. Scope and tailor security controls
    C. Take inventory
    D. Develop an information security strategy

    ☞ Answer to QOTD: 20200705

63. **Your company decides to start the business of selling toys online and shipping globally. A team in-house is in charge of developing an E-Commerce system that supports the new business. The development team is conducting threat modeling to identify potential threats to the database.**

    Which of the following security control is least related to data at rest?

    A. Data classification
    B. Authorization
    C. Storage redundancy
    D. Data marking

    ☞ Answer to QOTD: 20191117

64. **You are the CISO working for a direct bank based in Taiwan that relies entirely on internet banking. You are preparing the data policy and considering the data classification scheme. You prefer the classification criteria that cover widespread concerns.**

Which of the following classification criteria best meets your requirement?

A. Sensitivity
B. Criticality
C. Business value
D. Recovery cost

☞ Answer to QOTD: 20200107

65. **A USB dongle used by an engineer in the R&D department lost on the ground is found without a physical label identifying the sensitivity of the information contained. According to the data policy, all storage media shall be labeled.**

Which of the following action should be taken first?

A. Label the USB dongle at the highest level of sensibility
B. Classify and label the USB dongle as initial level
C. Examine the USB dongle on a secured workstation and label it based on the result
D. Inform the owner of the USB dongle and ask him to label it

☞ Answer to QOTD: 20200210

DATA LIFE CYCLE

66. **Your company decides to start the business of selling toys online and shipping globally. The E-Commerce system that supports the new business will be developed in-house. The solution architect chooses to implement a RAID storage system composed of high-capacity and high-speed Solid-State Disks (SSD). The development team is developing a security plan for the system.**

    Given security is a priority concern, which of the following is the best to deal with issues of data remanence when retiring disks or the storage system?

    A. Degaussing
    B. Low-level formatting
    C. Multiple passes of overwriting
    D. Cryptographic Erase

    ☞ Answer to QOTD: 20191101

67. **A desktop personal computer with an ATA hard drive used by an engineer in the R&D department is going to be retired. According to the media marking policy, the hard drive with confidential data shall be purged so as not to be recovered. Which of the following sanitization operation cannot meet the requirement?**

    A. Use the block erase method
    B. Write zeros in all bytes of logical sectors
    C. Overwrite the internal media with a constant value
    D. Change the internal encryption keys that are used for user data

    ☞ Answer to QOTD: 20200209

68. **Organizations should keep data only as long as it is required. To reduce the volume of data stored and ensure that only relevant data is preserved, which of the following is the least consideration?**

A. Data location
B. Data types
C. Strength of cryptographic algorithms
D. Retention period

☞ Answer to QOTD: 20200211

69. **Your organization shall preserve accounting transactions for at least ten years per regulatory requirements.**

After conducting data analytics, you discover that transactions stored in the database for more than one year and might be reused or queried account for 5% only.

Which of the following is the least concern in terms of enforcing the regulatory mandate?

A. Hierarchical storage management (HSM)
B. Data retention policy
C. Backup validation
D. Offsite tape vaulting

☞ Answer to QOTD: 20200220

70. **Your company is selling toys online and ships globally. The business has been supported by a 3-tier web system for around four years.**

The database server is equipped with a RAID 5 storage, to improve transaction performance, composed of three 1TB SSDs (solid-state drive) with

three years of MTBF (mean time between failure) and warranty.

The newly recruited system administrator is planning to replace the SSDs with new ones in higher capacity. The customer data in the database is classified as confidential.

Which of the following is the best way to address this issue?

A. Consult the information system owner
B. Destroy the media to avoid disclosure of information
C. Engage the maintenance provider and exchange the SSDs for warranty or cost rebate
D. Upgrade the RAID storage to five 2TB SSDs with 5 years of MTBF

☞ Answer to QOTD: 20191001

SECURITY CONTROL TAXONOMY

71. **The HIPAA Security Rule defines certain safeguards as "the technology and the policy and procedures for its use that protect electronic protected health information and control access to it."**

    Which of the following best describes the category or type of the safeguard mentioned above?

    A. Directive
    B. Management
    C. Technical
    D. Logical

    ☞ Answer to QOTD: 20191221

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

SECURITY ENGINEERING APPROACHES

72. **Your company decides to start the business of selling toys online and shipping globally.**

    A team in-house is in charge of developing an E-Commerce system that supports the new business.

    The project team is evaluating secure information system development processes to follow.

    Which of the following is least applicable to the system engineering for this project?

    A. System Security Engineering Capability Maturity Model (SSE-CMM).
    B. INCOSE Systems Engineering Handbook
    C. NIST SP 800-160 (Systems Security Engineering)
    D. ISO/IEC/IEEE 15288 (Systems and software engineering — System life cycle processes)

    ☞ Answer to QOTD: 20191120

73. **Your company is engineering an information system to support the new business of selling toys online. As a security professional, you recommend following the ISO/IEC/IEEE 15288 standard (Systems and software engineering – System life cycle processes) to ensure the use of secure information system development processes. You also emphasize that "Information Management" is one of the most critical processes.**

    To which of the following process families does the "Information Management" belong?

    A. Agreement Processes
    B. Organizational Project-Enabling Processes

C. Technical Management Processes
D. Technical Processes

☞ Answer to QOTD: 20190830

74. **To address security concerns, you align the software development life cycle to ISO 15288, which consists of four families or groups of system life cycle processes: agreement, organizational project-enabling, technical management, and technical processes.**

Which of the following belongs to the process family, Technical Processes?

A. Configuration Management
B. Life Cycle Model Management
C. Quality Assurance
D. Business or Mission Analysis

☞ Answer to QOTD: 20200128

75. **Your company is awarded a contract to develop a customized firewall product for a well-known brand security company. As a security professional, you are a member of the integrated product team. After a workshop for collection and elicitation of protection needs from the customer and stakeholders, you finished specifying security functional and assurance requirements.**

Which of the following activities conducted by the quality assurance team ensures the product compliant with the specifications?

A. Certification
B. Accreditation
C. Verification
D. Validation

☞ Answer to QOTD: 20200623

76. **Your customer sells toys online worldwide. A web-based E-Commerce system developed in-house supports the business. The payment gateway of the EC system is outsourced to your company as a software project.**

Your company has won the bid, which of the following is the best methodology, approach, or framework that provides specific stages, processes, and roles and responsibilities to guide your software development?

A. Capability Maturity Model Integration (CMMI)
B. The NIST SDLC Model
C. The NIST Risk Management Framework (RMF)
D. The Unified Software Development Process

☞ Answer to QOTD: 20200611

SYSTEM LIFE CYCLE AND RMF

77. **Your company is engineering an information system to support the new business of selling toys online. As a security professional, in which phase should you ensure the use of secure information system development processes according to the System Development Life Cycle (SDLC) from the National Institute of Standards and Technology (NIST)?**

    A. Initiation
    B. Development/Acquisition
    C. Implementation/Assessment
    D. Operations and Maintenance

    ☞ Answer to QOTD: 20190901

78. **Your company decides to start the business of selling toys online and shipping globally. A team in-house is in charge of developing an E-Commerce system that supports the new business. As a security professional, you are conducting a privacy impact assessment according to the standard, ISO 29134 – Guidelines for Privacy Impact Assessment, while other team members are in charge of other project work.**

    Which of the following is least likely to happen at this stage?

    A. Scope and tailor security controls
    B. Categorize the E-Commerce system
    C. Assess business impact
    D. Ensure the use of secure SDLC processes

    ☞ Answer to QOTD: 20191110

79. **Your company decides to start the business of selling toys online and shipping globally. A team in-house is in charge of developing an E-Commerce system that supports the new business. The project team has finished business and privacy impact analysis.**

Which of the following security activity should be conducted next?

A. Assess system security
B. Create a detailed plan for certification and accreditation (C&A)
C. Assess risk to the system
D. Review operational readiness

☞ Answer to QOTD: 20191126

80. **Your company decides to start the business of selling toys online and shipping globally. The E-Commerce system that supports the new business will be developed in-house. The software development project has just been kicked off for a couple of days, and you are preparing for the project meeting tomorrow.**

As a security professional, which of the following should you consider first?

A. Risks to the system
B. Impact of privacy breach
C. System Security Architecture
D. Stakeholders protection needs and requirements

☞ Answer to QOTD: 20191011

81. **Your company decided to go for the ISO 27001 certification. After conducting the risk assessment, you are identifying controls to mitigate the risks.**

To meet the requirements of the standard, you prepared a statement of applicability, which includes all the controls recommended by Annex A of the standard, merged the identified controls into the statement, and provided a justification for each included or excluded control.

Which of the following best describes this process?

A. Categorization and Classification
B. Verification and Validation
C. Certification and Accreditation
D. Scoping and Tailoring

☞ Answer to QOTD: 20190914

82. **According to the NIST SDLC, which of the following is the first security activity that should be conducted before authorizing an information system to operate?**

A. Assess risk to the system
B. Assess business impact
C. Assess system security
D. Review operational readiness

☞ Answer to QOTD: 20200411

83. **You are the system owner of the newly implemented Transportation Management System in your organization. You have compiled a package of documentation for authorization to operate (ATO).**

Which of the following is least likely to be included in the authorization package?

A. Risk Management Strategy
B. Security and privacy plans
C. Security and privacy assessment reports
D. Executive summary

☞ Answer to QOTD: 20200206

84. **In the NIST Risk Management Framework (RMF), authorization is the process by which a senior management official, the authorizing official, reviews security and privacy information describing the current security and privacy posture of information systems or common controls that are inherited by systems.**

Which of the following is not an authorization decision of the process?

A. Authorization to operate
B. Ongoing authorization
C. Denial of authorization
D. Common control authorization

☞ Answer to QOTD: 20200418

85. **Your company decides to subscribe to SaaS from a well-known cloud service provider. As a security professional, you are tasked to prepare for a security plan.**

Which of the following should you do first?

A. Determine data types processed by the SaaS cloud services.
B. Categorize the system based on its impact level
C. Scope and tailor security controls
D. Identify stakeholders

☞ Answer to QOTD: 20200630

86. **Your company is engineering an information system (the system) to support the new business of selling toys online. As a security professional, you are a**

member of the engineering project team and responsible for ensuring the security needs are addressed properly, and the information system is compliant with the security policies in your company. The project was kicked off last week.

Which of the following should be determined first?

A. Categorize the system based on the impact if it is compromised
B. Select appropriate security controls from certain control frameworks
C. Scope and tailor the security controls based on business requirements
D. Evaluate the value of the data processed by the system and the impact in case the data is breached

☞ Answer to QOTD: 20190827

87. **You are the CISO working for a direct bank based in Taiwan that relies entirely on internet banking. You are referencing the NIST Risk Management Framework (RMF) to determine security controls for the core banking system.**

Which of the following best describes the criteria on which the control selection process depends?

A. The impact level of the system
B. Information types the system processes
C. The sensitivity of information the system processes
D. The value of the information the system processes

☞ Answer to QOTD: 20200105

88. **Your company is implementing the ERP system. As a security professional, you are selecting security controls as a baseline from a well-known security control framework and customizing it according to**

your company's specific requirements and constraints.

Which of the following is the least concern during the process of scoping and tailoring?

A. Compensating controls
B. Common controls
C. The impact level of the ERP system
D. Certification and accreditation

☞ Answer to QOTD: 20200620

ARCHITECTURAL COMPONENTS

89. **Your company decides to start the business of selling toys online and shipping globally. A team in-house is in charge of developing an E-Commerce system that supports the new business.**

    The development team encrypts the database connection string used in the application server cluster as it contains credentials, and stores the cyphertext in the configuration file using AES.

    The development team shall use the trusted platform module (TPM) on each application server to protect the AES cryptographic key without platform measurement.

    Which of the following is the best solution?

    A. Key Signing
    B. Key Binding
    C. Key Sealing
    D. Key Clustering

    ☞ Answer to QOTD: 20191116

90. **Your company decides to start the business of selling toys online and shipping globally. The E-Commerce system that supports the new business will be developed in-house. The development team is evaluating the software runtime environment of the client with security concerns as the first priority.**

    Which of the following is the most secure or restrictive environment in terms of the confinement and bound issues?

A. Application Runtime Framework (e.g., JVM or .NET)
B. Modern Web Browser
C. Bare metal hypervisor (Type I)
D. Hosted hypervisor (Type II)

☞ Answer to QOTD: 20191002

91. **Buffer overflow is one of the most common attacks. Which of the following does the "buffer" mean?**

A. Small memories on or close to the CPU, e.g., cache or registers
B. Areas of the main memory, e.g., stack or heap
C. The embedded memory in a hard disk drive
D. The memory reserved for DNS entries

☞ Answer to QOTD: 20200329

92. **A program needs to load the value 0x30, stored in memory address #100, into the processor register AX for processing. The assembly code looks like, LD AX,#100.**

Which of the following the memory addressing modes does the assembly code demonstrate?

A. Immediate addressing
B. Register addressing
C. Direct addressing
D. Indirect addressing

☞ Answer to QOTD: 20200413

SECURITY POLICIES AND MODELS

93. **Your organization implements mandatory access control based on the Bell-LaPadula Model, which doesn't support the strong star property, an alternative to the star property.**

    There is a printer, classified as Top Secret, in your organization.

    Bob is a middle officer with a security clearance of Secret. He is also assigned both the simple and star security property defined in the Bell-LaPadula Model.

    Can Bob print his report to the printer classified as Top Secret?

    A. Yes, Bell-LaPadula Model does not prohibit this type of information flow.
    B. Yes, Bell-LaPadula Model allows reading data from the upper level of sensitivity.
    C. No. Bell-LaPadula Model prohibits reading data from the upper level of sensitivity.
    D. No. Bell-LaPadula Model prohibits writing data to a lower level of sensitivity.

    ☞ Answer to QOTD: 20190828

94. **Your organization implements the multi-level mandatory access control, which is based on the Bell-LaPadula model. An employee with "Secret" clearance complained that he could not write to a file classified as "Top Secret."**

    Which of the following is the most likely reason?

A. The employee is assigned the * (star) Property
B. The employee is not assigned the Simple Security Property
C. The employee and the file belong to the different lattice of need-to-know
D. The employee is under a race condition against the file locked by another user

☞ Answer to QOTD: 20191014

95. **You are working for an organization in which every employee is granted a security clearance after completion of a thorough background check, and assets are labeled after the classification process. Your access to classified resources is authorized based on if your security level dominates that of the resource. You are not allowed to write data to a lower security level.**

Which of the following may concern your organization most?

A. Biba Model
B. Integrity
C. Bell-LaPadula Model
D. Confidentiality

☞ Answer to QOTD: 20190909

96. **You are working for an organization in which every employee is granted a security clearance after completion of a thorough background check, and assets are labeled after the classification process.**

Your access to classified resources is authorized based on if your security level dominates that of the resource. You are not allowed to write data to a lower security level.

Which of the following is least related to the access control model of the organization?

A. State Machine
B. Information Flow
C. The * (star) Integrity Axiom
D. Lattice Model

☞ Answer to QOTD: 20190910

97. **You were working for a law firm and tasked to evaluate access control models for information systems. It is a major concern that your law firm may represent both sides in an ongoing legal case, and the information flow between the two legal teams may result in collusion or bias.**

Which of the following is the best fit for your firm?

A. Clark-Wilson Model
B. Graham-Denning Model
C. Take-Grant Model
D. Brewer-Nash Model

☞ Answer to QOTD: 20190906

98. **Your company finished conducting an asset inventory. As the head of the sales department, you are assigned as the data owner of the customer master data, which you then classified as privacy according to the classification scheme. You are now authorizing employees to access the customer data based on their duty.**

Which of the following security models is most likely used to support the task?

A. Clark-Wilson Model
B. Take-Grant Model

C. Biba Model
D. Brewer and Nash Model

☞ Answer to QOTD: 20190928

99. **Your company decides to sell toys online and ships globally. An in-house team is responsible for developing the online shopping website. A customer's sales order is stored in a master table and several detail tables.**

Which of the following is least related to the data integrity across relations?

A. Clark-Wilson Model
B. ACID (Atomicity, Consistency, Isolation, Durability)
C. Entity Integrity
D. Referential Integrity

☞ Answer to QOTD: 20200318

100. **Your company sells toys online worldwide. The sales manager, as a data owner, is granting privileges of access to the customer profiles to Alice.**

Which of the following is the best security model that supports access control and enforces confidentiality?

A. Graham-Denning Model
B. Clark-Wilson Model
C. Biba Model
D. Bell-LaPadula model

☞ Answer to QOTD: 20200512

101. **Your company sells toys around the world. You are developing an EC system supported by an RDBMS and write the following SQL code to create a sales order:**

01 Begin Transaction
02 Insert Orders(Id, CustomerId, OrderDate) Values(1, 1, '2020/08/15');
03 Insert OrderItems(Id, OrderId, ProductId, Quantity, Price) Values(1, 1, 1, 1, 9.9);
04 Commit Transaction

From the perspective of the Clark-Wilson model, which of the following best describes the entity, Sales Order, expressed in the SQL code?

A. Transformation Procedures (TPs)
B. Integrity Verification Procedure (IVP)
C. Constrained Data Item (CDI)
D. Unconstrained Data Item (UDI)

☞ Answer to QOTD: 20200815

102. **Eve spying undercover as an employee was cleared as Secret and imposed with the *-security (star) property. She printed a classified document to a printer labeled as Confidential. After printing two pages of the document, the printer ran out of paper.**

Which of the following best describes the printing work?

A. Eve's clearance dominates that of the printer.
B. The collection of the printer's non-hierarchical categories is a superset of Eve's.
C. Eve controls a covert channel to the printer.
D. A trusted channel is established between Eve and the printer.

☞ Answer to QOTD: 20200617

103. **Eve was cleared as Top Secret and printed a classified document to a printer. The printer sent a success**

notification to Eve after printing. The printout has an explicit expression, //TS//SCI, on the header.

Which of the following is not true?

A. The printed document is labeled as //TS and compartmented as //SCI.
B. Eve has need-to-know of the classified document in the performance of her duties.
C. Eve's security level dominates that of the classified document.
D. Eve's security level is higher than or equal to that of the printer.

☞ Answer to QOTD: 20200618

EVALUATION AND ASSURANCE

104. **Your organization decides to purchase new firewalls to replace the legacy ones. Two brand vendors are competing for the bid.**

Which of the following is the best evidence of your organizational capability that assures the procurement decision of firewalls renders the best outcome?

A. Common Criteria (CC)
B. Service Organization Controls (SOC) 2 Type 2 Report
C. Capability Maturity Model Integration (CMMI)
D. Evaluation Assurance Level (EAL)

☞ Answer to QOTD: 20200421

105. **Your company is procuring computer systems to support the new business of video streaming services. You are responsible for ensuring the computer systems are compliant with the security policies in your company.**

Which of the following is your most concern?

A. Trusted Computing Base
B. System Design Flaws
C. Security Kernel
D. Implicit Covert Channels

☞ Answer to QOTD: 20190822

106. **Your company decides to start the business of selling toys online and shipping globally. The E-Commerce system that supports the new business will be developed in-house. The development of some software modules will be outsourced to external**

software vendors. The computer systems, operating systems, and other standard hardware and essential software will be procured as well. Which of the following is least related to the procurement of this project?

A. Common Criteria
B. Vender's reputation
C. Zachman Enterprise Framework
D. The Capability Maturity Model Integration (CMMI)

☞ Answer to QOTD: 20191031

107. **Your company is implementing solutions to support salespeople as road warriors and boost sales. Laptops, mobile phones, VPN, wireless networks, and customer relationship management (CRM) systems are parts of the selected solution. As a security professional, you are helping review vendors. Which of the following vendor or provider is the least trusted?**

A. The software provider providing self-assessed security results
B. The integration service provider registered in a well-known industrial directory
C. The vendor specified or mandated by the senior management
D. The maintenance service provider having provided services for years

☞ Answer to QOTD: 20200202

108. **Your company sells toys online worldwide. A web-based E-Commerce system developed in-house and deployed to a public cloud supports the business. The EC system accepts credit cards and processes personal data.**

Which of the following addresses those concerns and provides the best assurance?

A. PCI-DSS
B. Risk Assessment
C. Security Assessment
D. Third-party Audit

☞ Answer to QOTD: 20200530

109. **Your company develops security products. You are the head of the firewall product line and studying well-known evaluation criteria for your products, e.g., TCSEC, ITSEC, Common Criteria, etc.**

Which of the following is least preferable as the objectives of the evaluation criteria?

A. To provide guidance for manufacturers to build trustworthy products
B. To provide users with a yardstick to assess the degree of trust of your products
C. To benchmark products in terms of cost/benefit to inform procurement decisions
D. To provide a basis for specifying security requirements in acquisition specifications

☞ Answer to QOTD: 20200616

110. **Your company develops security products and competes in the market with the first-mover strategy. Time-to-market and third-party assurance, e.g., Common Criteria, are critical success factors. You lead the firewall development team.**

Which of the following does not belong to assurance requirements defined in Common Criteria?

A. Non-repudiation of origin
B. Security architecture
C. Functional specification
D. Security policy modeling

☞ Answer to QOTD: 20200615

111. **Your company decides to start the business of selling toys online and shipping globally. A team in-house is in charge of developing an E-Commerce system that supports the new business. Network security solutions include devices like firewalls, IPS, SIEM, and so forth.**

Which of the following is the most helpful in the procurement decision and communication to the management?

A. Security Target (ST)
B. Evaluation Assurance Level (EAL)
C. Target of Evaluation (TOE)
D. Protection Profile (PP)

☞ Answer to QOTD: 20191111

112. **Firewalls are one of your company's product lines. You are responsible for submitting a new web application firewall (WAF) that supports large scale web traffic for certification against the Common Criteria (CC) to get an Evaluation Assurance Level (EAL). You have sent the product as Target of Evaluation (TOE), Security Target (ST), and related documentation to an approved CC laboratory for certification. After waiting for a prolonged period of four months, you finally received a CC certification report. Which of the following EAL is most likely?**

A. EAL 1
B. EAL 2
C. EAL 2+
D. EAL 3

☞ Answer to QOTD: 20191113

113. **Firewalls are one of your company's product lines. You submitted a new web application firewall (WAF) that supports large scale web traffic to an approved CC testing laboratory for certification as a Common Criteria (CC) Evaluation Assurance Level 4 (EAL4) product. You have sent the product as Target of Evaluation (TOE), Security Target (ST), and related documentation to an approved CC testing laboratory for certification.**

Which of the following is least likely evaluated?

A. Security Target (ST)
B. Target of Evaluation (TOE)
C. Operational Environment
D. Guidance documents

☞ Answer to QOTD: 20191114

114. **Your company develops security products and competes in the market with the first-mover strategy. Time-to-market and third-party assurance, e.g., Common Criteria, are critical success factors. You lead the firewall development team.**

Which of the following is the least priority for the development of a new firewall model?

A. Documentation
B. Management commitment
C. Assurance with a formal design
D. Selection of computer languages

☞ Answer to QOTD: 20200614

115. **Your company is a well-known security product manufacturer. You are in charge of the Security Information and Event Management (SIEM) product line that receives logs from other security products.**

To protect the transmission of log between the SIEM server and other security products, which of the following security function should be implemented?

A. Security perimeter
B. Trusted Computing Base (TCB)
C. Trusted path
D. Trusted channel

☞ Answer to QOTD: 20200517

116. **Your company sells toys online worldwide, which is supported by a three-tiered E-Commerce web-based system.**

You are planning for patching the web servers and worried about the integrity of system configurations is compromised if failures occur when applying patches.

Which of the following security functional components best addresses your concerns?

A. Reference monitor
B. Trusted path
C. Configuration management
D. Manual recovery

☞ Answer to QOTD: 20200515

CLOUD COMPUTING

117. **A cloud provider provides cloud services to cloud consumers. Which of the following does not belong to the service models of the cloud provider?**

A. Virtual machines without pre-installed operating systems
B. Platforms which cloud consumers can upload applications
C. Services that are publicly available
D. E-mail services through the web interface

☞ Answer to QOTD: 20200409

118. **Your company is a well-known cloud services provider. A cloud storage solution is sold to consumers as SaaS. As a security professional, you identified the risk that individuals might store copyrighted materials on cloud storage and violate intellectual property laws.**

Which of the following is the most appropriate risk mitigation strategy?

A. Remove copyrighted materials immediately if the risk has materialized.
B. Capture the copyrighted materials as evidence to present to the court.
C. Leave copyrighted materials intact as those who uploaded them are responsible.
D. Conduct digital forensics and preserve the evidence chain of custody.

☞ Answer to QOTD: 20200503

119. **Your company decides to start the business of selling toys online and shipping globally.**

A team in-house is in charge of developing an E-Commerce system that supports the new business. The solution will be deployed using a PaaS in a public cloud.

As a security professional, you are assessing the risk of cloud service. Which of the following is the least concern?

A. Lock-in
B. Lock-out
C. Lack of audit rights
D. Shared responsibility

☞ Answer to QOTD: 20191112

CRYPTOGRAPHY

120. **Alice is tasked to evaluate and implement a cryptographic solution to protect the company's classified data at rest, in motion, and in use across the data life cycle. She decides to use a hybrid strategy, that is, the synergy of symmetric and asymmetric cryptography. The asymmetric cryptography is used for symmetric key exchange and digital signature, while the data is protected by symmetric cryptography. Which of the following is the most unlikely to achieve in terms of her strategy?**

A. Confidentiality
B. Integrity
C. Availability
D. Non-repudiation

☞ Answer to QOTD: 20190905

121. **Alice works for a company where the public key infrastructure is implemented. She sent an encrypted message to Bob. Which of the following is the most likely reason why she employed the AES secret key to encrypt the message instead of her RSA public key?**

A. The performance of AES is faster if the work factor is the same
B. The requirement for AES key length is shorter if the work factor is the same
C. The encryption by the AES secret key is more effective if key exchange is secured
D. The computational complexity for breaking AES is higher if the key length is the same

☞ Answer to QOTD: 20200719

122. **You are actively engaging in the open-source community of cryptography and reviewing the source code of a stream cipher to implement on mobile apps.**

Which of the following is the best justification for selecting the open-source cipher instead of AES?

A. Shorter key length
B. Lower requirement for hardware capacity
C. Stronger work factor
D. Open design

☞ Answer to QOTD: 20200727

☐ Open Design and Cipher Selection

123. **Alice is sending an encrypted message to Bob. According to Kerckhoffs' principle, which of the following must be kept secret?**

A. The cipher mode of operation
B. The unique random value used once to avoid repeating patterns
C. The input used to confuse the relationship with the ciphertext
D. The key used to encrypt data that can only be decrypted by another key

☞ Answer to QOTD: 20200718

124. **In cryptography, an initialization vector (IV) can achieve semantic security, a property whereby the encryption under the same key does not generate repeated patterns so that an attacker cannot infer relationships between plaintext and ciphertext.**

Which of the following statements about IV is not true?

A. IV is an arbitrary number that is used only once.
B. IV must be protected to the extent which is as secure as the secret key.
C. An incorrect IV used for decryption in CBC mode causes only the first block of plaintext to be corrupted, not the remaining.
D. Counter (CTR) mode turns a block cipher into a stream cipher and doesn't employ an IV in the strict sense.

☞ Answer to QOTD: 20200405

125. **You are sniffing network traffic as a middle man and have captured a user's encrypted login session for a couple of days. After analyzing the session packets, you conclude that the symmetric block cipher encrypts them. However, you are confused that the ciphertext of the password varies even though the user's password is not changed.**

Which of the following is the least likely cipher mode of operation used to protect the user login session?

A. Electronic Codebook (ECB)
B. Cipher Block Chaining (CBC)
C. Cipher Feedback (CFB)
D. Output Feedback (OFB)

☞ Answer to QOTD: 20200305

126. **You are evaluating cryptographic algorithms to secure your order processing. Three block-ciphers, RC6, Rijndael, and Twofish, are on the final list after the first round of evaluation.**

Which of the following terminologies is least likely used in the evaluation process?

A. IV
B. Salt

C. Nonce
D. Entropy

☞ Answer to QOTD: 20200713

127. **Your company develops web conferencing products. You are the head of the research and development department.**

You plan to provide end-to-end protection over user sessions based on the symmetric cipher. An open design, work factor of cryptanalysis, and user acceptance are major evaluation criteria.

Which of the following is the least appropriate cipher?

A. Rijndael
B. Skipjack
C. RSA RC6
D. Serpent

☞ Answer to QOTD: 20200625

128. **You are evaluating cryptographic algorithms to secure your order processing. Three block-ciphers, RC6, Rijndael, and Twofish, are on the final list after the first round of evaluation.**

Which of the following is the least concern to select the finalist?

A. Avalanche effect
B. Work factor
C. Key exchange
D. Confusion and diffusion

☞ Answer to QOTD: 20200712

☐ Confusion and Diffusion

129. **Symmetric ciphers encrypt plaintext into ciphertext using a secret key. Confusion and diffusion are two cryptographic properties of a cipher to make cryptanalysis difficult.**

    Which of the following statements is not true?

    A. Substitution algorithms support confusion
    B. Confusion applies to both stream and block cipher
    C. Confusion makes recovering the secret key by the ciphertext-only attack more difficult
    D. Confusion reduces patterns and obscures the relationship between plaintext and ciphertext

    ☞ Answer to QOTD: 20200304

130. **Symmetric ciphers encrypt plaintext into ciphertext using a secret key. Confusion and diffusion are two cryptographic properties of a cipher to make cryptanalysis difficult.**

    Which of the following statements is not true?

    A. Diffusion makes cryptographic attacks more difficult
    B. Diffusion obscures the relationship between plaintext and ciphertext
    C. Transposition algorithms and P-Box support diffusion
    D. Diffusion applies to stream cipher only

    ☞ Answer to QOTD: 20200308

131. **You are conducting cryptanalysis to a symmetric cipher. You have access to the ciphertext in transit. You realize the secret key is not static but replaced with a new one periodically.**

Which of the following is the most likely effect you are facing because of the ever-changing secret key and ciphertext?

A. Confusion
B. Ciphertext-only attack
C. Chosen-ciphertext attack
D. Diffusion

☞ Answer to QOTD: 20200714

132. **You are taking the cryptography course and working on the homework to develop a cipher. Which of the following is the best technique to complicate the ciphertext if any alternation of bits in plaintext occurs?**

A. XOR
B. ROT-3
C. Table lookup
D. Rotation of bits

☞ Answer to QOTD: 20200720

133. **Confusion and diffusion are two properties of the operation of a secure cipher. Confusion refers to making the relationship between the ciphertext and the encryption key as complex and involved as possible; diffusion refers to dissipating the statistical structure of plaintext over the bulk of ciphertext.**

Which of the following is least used in confusion and diffusion?

A. Logarithm
B. Permutation
C. Exclusive OR
D. Table lookup

☞ Answer to QOTD: 20190918

☐ Key Generation and Exchange

134. **You are developing a client/server-based application in which the client shall communicate with the server through a trusted channel supported by symmetric encryption. Secret keys shall be generated and changed periodically to secure communication.**

Which of the following is the best design to generate secret keys in terms of scalability and the work factor?

A. The client using a pseudorandom number generator (PRNG)
B. The client employing the onboard cryptoprocessor
C. The server invoking the operating system's API
D. The server utilizing the hardware security module

☞ Answer to QOTD: 20200723

135. **You are developing a client/server-based application where clients shall communicate with peer clients and the server based on the public key infrastructure. There are ten clients on the network.**

Which of the following is the required number of secret keys among clients and the server?

A. 11
B. 22
C. 55
D. 77

☞ Answer to QOTD: 20200724

136. **Alice and Bob are students with a major in Computer Science, taking the Cryptography course this semester. They turned in the homework of implementing a 128-bit cryptographic key generator**

graded in terms of entropy. Alice received an A, while Bob received a B.

Why did the professor grade so?

A. Alice's generates keys faster than Bob's
B. The entropy values of Alice and Bob are 0.970950594 and 0.992774454 respectively
C. Alice used mouse movements to generate randomness, while Bob used standard Operating System-level Application Programming Interface (API) functions
D. Alice's keyspace is larger than Bob's.

☞ Answer to QOTD: 20191209

137. **Alice encrypted a document using AES with an encryption key that is a combination of her birthday and phone number. She has sent the document to bob through e-mail and is considering how to deliver the key securely.**

Which of the following is the least feasible?

A. Print the key out and send it through a courier
B. Text the key using WhatsApp
C. Mail him a one-time password token to generate the key
D. Send the key encrypted by Bob's public key through email

☞ Answer to QOTD: 20191217

138. **You are developing a client/server-based application in which the client shall communicate with the server through a trusted channel supported by symmetric encryption.**

Which of the following is least likely employed to exchange or distribute the predefined secret key?

A. Human brain
B. Diffie-Hellman
C. Public Key Encryption
D. USB flash drive dongle

☞ Answer to QOTD: 20200722

139. **You are developing a client/server-based application in which the client shall communicate with the server through a trusted channel.**

Which of the following is the best design of key exchange to encrypt data in transit?

A. The client encrypts the preshared key using its private key
B. The client encrypts the premaster key using the server's private key
C. The client encrypts the session key using the server's public key
D. The client encrypts the master key using the server's public key

☞ Answer to QOTD: 20200721

140. **A client generates a session key randomly, encrypts it using a server's public key, and sends it to the server, which decrypts the session key using its private key to initiate a secure channel.**

Which of the following best describes this process?

A. Diffie-Hellman
B. Key agreement
C. Key exchange
D. Authentication

☞ Answer to QOTD: 20200820

☐ Asymmetric Encryption

141. **You are developing a client/server-based application where the client shall communicate with the server through the public key infrastructure.**

Which of the following asymmetric algorithms is not developed based on the discrete logarithm?

A. RSA
B. ElGamal
C. Diffie-Hellman
D. Elliptic-Curve Cryptography (ECC)

☞ Answer to QOTD: 20200819

142. **Alice generated a public/private key pair for asymmetric cryptography. She sent Bob a document with a message digest encrypted by her private key. Bob then validated the document by computing a new message digest from the document and comparing it with the decrypted message digest. If the comparison matches, Bob can assure that the document comes from Alice while she cannot deny it.**

Which of the following best describes the security principle or objective the process will achieve?

A. Integrity
B. Authenticity
C. Non-repudiation
D. Accountability

☞ Answer to QOTD: 20190907

143. **Alice generated a public/private key pair for asymmetric cryptography. She sent Bob a document with a message digest encrypted by her private key. Bob then validated the document by computing a new**

message digest from the document and comparing it with the decrypted message digest. If the comparison matches, Bob can assure that the document comes from Alice while she cannot deny it.

Which of the following best describes the process when taking technical and legal aspects into account?

A. Electronic Signature
B. Authenticity
C. Digital signature
D. Non-repudiation

☞ Answer to QOTD: 20190903

144. **To increase the work factor against cryptoanalysis or cryptographic attacks, Alice generated an RSA public/private key pair with a key size of 3072 bits, equivalent in strength to 128-bit symmetric keys, for asymmetric cryptography. She sent to bob a document encrypted by her private key. However, she didn't sign the document. Once the encrypted document is received, Bob then decrypts the document by her public key.**

To which of the following will the process most likely lead?

A. Integrity
B. Confidentiality
C. Non-repudiation
D. Data breach

☞ Answer to QOTD: 20190904

145. **Your organization decides to implement the security functionality of the digital signature on the email system based on the public key infrastructure.**

Which of the following statements is not true about the initiative?

A. Certificate Authorities (CAs) are required
B. The email message is encrypted by the public key of the recipient
C. Both data integrity and sender identity can be assured
D. Only the digest of the email message is encrypted by the private key of the sender

☞ Answer to QOTD: 20200215

146. **Your company decides to start the business of selling toys online and shipping globally. The E-Commerce system that supports the new business will be developed in-house. The development team is evaluating the secure transmission solution between browsers and the webserver to protect data in motion.**

Which of the following the best strategy?

A. Security through obscurity
B. Web of trust
C. Chain of trust
D. Shared key encryption

☞ Answer to QOTD: 20191103

☐ Hash and MAC

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

NETWORK ESSENTIALS

151. **You are designing and implementing the company network for a startup.**

Which of the following is least related to the Network layer?

A. Determine the scale of a network
B. Identify and number hosts
C. Name hosts and networks
D. Select the transmission path

☞ Answer to QOTD: 20200604

152. **You are considering solutions to connect multiple branches to the headquarters. You select MPLS and RIP as the solution in the end.**

Which layers are the protocols between in terms of the ISO OSI model?

A. Data Link, Network
B. Transport, Physical
C. Data Link, Internet
D. Network, Transport

☞ Answer to QOTD: 20200131

153. **Your company is constructing a new building with a structured cable system topology per the standard EIA/TIA 568.**

As a network engineer, you are designing an 802.3 network. The vertical backbone between floors is connected with optical cables. The horizontal cabling is implemented with Category 5e UTP.

Which of the following is the most concern?

A. Near-end Crosstalk (NEXT) between floors
B. Attenuation after signal transitioning by active hubs
C. Contention on media access
D. Loss of token and frames on high traffic transmission

☞ Answer to QOTD: 20200319

154. **You are implementing the company networks for a startup. Which of the following is least related to the data link layer?**

A. Configuring the physical address of a network interface card.
B. Implementing a linear network with token passing.
C. Splitting traffic by VLAN tagging.
D. Binding multiple logical addresses to a network interface card.

☞ Answer to QOTD: 20200601

155. **A desktop computer sends an IP packet to the destination, 192.168.1.15/28. Which of the following devices most likely ignores or drops the packet?**

A. Bridge
B. Switch hub
C. Router
D. Firewall

☞ Answer to QOTD: 20200328

156. **As a CISSP aspirant, you are studying the network concepts. Which of the following statement is true?**

A. Mobile devices running IP must have a routing table like a router to transmit data
B. Network nodes must execute routing protocols to transmit packets

C. IP, IPX, and NetBEUI are routed protocols supported by routers
D. Split horizon is a method to identify the minimum hop count

☞ Answer to QOTD: 20200111

157. **You are implementing the network for a small company where a bridge connects two network segments as a broadcast domain. The bridge maintains a MAC table or cache to make forwarding decisions.**

If TCP/IP is implemented to support network communication, which of the following is not true?

A. Hosts across the bridge must have the same subnet mask.
B. The network is vulnerable to sniffing attacks when the bridge reboots.
C. A router is required if two or more logical IP subnets are implemented.
D. Eavesdropping traffic across the bridge can result from cache overflow.

☞ Answer to QOTD: 20200602

158. **A host with an IP address, 10.10.10.6/29, sends ICMP control messages of Echo Request to 10.10.10.7/29 but receives no response because requests timed out.**

Which of the following is the most likely cause?

A. The destination ignores the requests, or the network is jammed.
B. The default gateway of the host is not properly configured.
C. The routing table of the gateway doesn't converge.
D. The destination resides in another broadcast domain.

☞ Answer to QOTD: 20200531

159. **You are implementing a company network for a startup. The IP address of the intranet is 192.168.1.0/24. You split the intranet into two subnets connected by a router: 192.168.1.0/25 and 192.168.128.0/25.**

Which of the following is the best for the router to forward IP packets from one subnet to the other?

A. Relay agent
B. Routing protocols
C. Routed protocols
D. Static routes

☞ Answer to QOTD: 20200619

160. **Users report connections to the enterprise information portal (EIP) often timed out because of poor network performance.**

As a security analyst, you suspect it can be resulted from denial-of-service (DOS) or distributed DOS (DOS) attacks. You connect your laptop to the mirror port of the core switching hub and start capturing traffic in promiscuous mode.

Which of the following attack targets is least likely to appear in the captured traffic?

A. 10.10.255.255/22
B. 10.10.254.0/22
C. 10.10.253.255/22
D. 10.10.252.0/22

☞ Answer to QOTD: 20200726

161. **Internet Protocol Security (IPsec) as a part of the Internet Protocol version 4 (IPv4) suite complements the Internet Protocol (IP).**

Which of the following cannot be achieved by IPsec?

A. Confidentiality
B. Detection and rejection of replays
C. Access control
D. Non-repudiation

☞ Answer to QOTD: 20200725

162. **You're implementing IPsec to protect data in transit. Which of the following is the least feasible through IPsec?**

A. Build a virtual data link over frame relay to connect two remote offices
B. Secure TFTP traffic that updates the firmware of network devices
C. Protect traffic between browsers and the enterprise information portal over LAN
D. Authenticate security gateways that establish the tunnel between two remote offices

☞ Answer to QOTD: 20200802

163. **Your company sells toys online and ships globally. After a customer is authenticated, the client browser receives the following HTTP response:**

```
HTTP/1.1 200 OK
Content-Type: application/json
{
  "sub": "VIP202003010001",
  "name": "Alice",
  "email": "alice@effectivecissp.com",
```

```
  "picture": "http://effectivecissp.com/i/alice.jpg"
}
```

If the HTTP response is encoded and rendered as a JSON Web Token (JWT) payload, which of the following layers of the ISO Open System Interconnection model best describes this design?

A. Application
B. Presentation
C. Session
D. Transport

☞ Answer to QOTD: 20200303

164. **Which of the following DNS operations is most likely to use the well-known port 53 to establish a connection?**

A. Iterative queries for MX records
B. Recursive queries for A records
C. DNSSEC resource records
D. Zone transfer

☞ Answer to QOTD: 20200414

165. **Alice frequently sends emails to Bob, which are split and encapsulated as IP packets transmitted through a series of intermediate nodes. However, the transmission path may vary because of the availability, quality, and bandwidth of circuits.**

Which of the following least affects the email transmission path?

A. DNS MX Records
B. Digital signature
C. Routing tables
D. Awareness training

☞ Answer to QOTD: 20200603

166. **Your company decides to start the business of selling toys online and shipping globally. The E-Commerce system that supports the new business will be developed in-house.**

To streamline the order fulfillment process, the system will be integrated with the ones of key business partners. The development team is evaluating solutions to exchange messages, e.g., XML or JSON, between systems in this supply chain integration initiative.

Which of the following layer of the ISO OSI reference model is most related to the evaluation?

A. Application
B. Message Exchange (MX)
C. Presentation
D. Transport

☞ Answer to QOTD: 20191025

167. **Converged protocols are the merging of specialty or proprietary protocols with standard protocols, such as those from the TCP/IP suite. FCoE, MPLS, iSCSI, and VoIP are common converged protocols.**

Which of the following is the protocol dealing with signaling in VoIP?

A. Real-time Transport Protocol (RTP)
B. Real-Time Streaming Protocol (RTSP)
C. Session Initiation Protocol (SIP)
D. Media Gateway Control Protocol (MGCP)

☞ Answer to QOTD: 20200401

168. **iSCSI is a standard for linking data storage facilities over an ordinary IP network to transport block-level data. A file server connects to a SAN (Storage Area Network) storage through iSCSI.**

Which of the following roles is the file server?

A. Initiator
B. Target
C. HBA (Host Bus Adapter)
D. NAS Client

☞ Answer to QOTD: 20200330

REMOTE ACCESS AND VPN

169. **You are designing a remote access solution to support sales representatives equipped with laptops, tablets, and smartphones as road warriors. Mobility, confidentiality, and integrity are your design objectives.**

Which of the following IPsec VPN solutions best meets your requirements?

A. IPsec Tunnel mode and AH protocol
B. IPsec Tunnel mode and ESP protocol
C. IPsec Transport mode and AH protocol
D. IPsec Transport mode and ESP protocol

☞ Answer to QOTD: 20200321

170. **You're implementing an L2TP/IPsec VPN solution to support remote employees. Which of the following is not true?**

A. AH may not be available in IPsec
B. AH ensures integrity only, but not confidentiality through encryption
C. Implementation of ESP is a mandatory requirement of IPsec
D. ESP ensures both confidentiality and the same level of integrity as AH does

☞ Answer to QOTD: 20200801

171. **You're implementing a VPN solution to connect a branch office to the headquarters through gateways with a T1 connection to the internet and ISDN BRI service as redundancy.**

Which of the following is least likely employed to authenticate VPN connections?

A. PAP
B. EAP-MD5
C. 802.1X
D. RADIUS

☞ Answer to QOTD: 20200803

WIRELESS NETWORKS AND WI-FI

172. **You bought a new mobile phone and tried to transfer contents from the old one using the transfer utility provided by the manufacturer. It transfers the contents via WIFI peer to peer without an access point.**

    Which of the following is most likely used for wireless identification?

    A. Automatic Private IP Addressing (APIPA)
    B. Private IP addresses defined in RFC 1918
    C. Media Access Control (MAC) Address
    D. Manufacturing series number

    ☞ Answer to QOTD: 20200325

173. **You bought a new wireless display adapter plugged in a TV set to which you can project your laptop screen for presentation. Your laptop connects to the adapter via WIFI peer to peer without an access point.**

    Which of the following modes is used for wireless transmission?

    A. Stand-alone mode
    B. Bridge mode
    C. Ad-hoc mode
    D. Wireless extension mode

    ☞ Answer to QOTD: 20200326

174. **Your company decides to implement remote conferencing and wireless screencasting in all the meeting rooms for efficiency and convenience.**

The wireless display transmitter and receiver, as a pair, work in the ad-hoc mode. Connections to Ethernet ports shall be authenticated through 802.1X. As a security professional, which of the following is the least concern?

A. Session-bombing
B. Ciphertext-only attack
C. Social engineering
D. Wiretapping

☞ Answer to QOTD: 20200523

175. **Wired Equivalent Privacy (WEP), ratified in 1997, is the first-generation security solution for 802.11 wireless networks.**

The 64-bit WEP uses the stream cipher RC4 with a 24-bit initialization vector (IV) and a 40-bit secret key. Hackers can use Aircrack-ng to sniff wireless traffic and crack the secret key by exploiting the short IV.

Which of the following best describes the attack used to break WEP?

A. Ciphertext-only
B. Known-plaintext
C. Chosen-plaintext
D. Chosen-ciphertext

☞ Answer to QOTD: 20200731

176. **TEMPEST (Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions) is about spying on information systems through leaking electromagnetic emanations, sounds, and mechanical vibrations and how to shield equipment against such spying.**

Which of the following is the most effective countermeasure against the concern of TEMPEST?

A. Captive portal
B. Awareness training
C. Air-gapped network
D. Wire-meshed space

☞ Answer to QOTD: 20200702

NETWORK ATTACKS

177. **Your company is constructing a new building with a structured cable system topology per the standard EIA/TIA 568. As a network engineer, you are designing an 802.3 network with hundreds of nodes.**

Which of the following is the least concern of your design?

A. Attenuation
B. ARP Attack (Address Resolution Protocol)
C. CAM Table Overflows (Content Addressable Memory)
D. Teardrop Attack

☞ Answer to QOTD: 20200322

178. **You are developing a network access control (NAC) solution to prevent unauthorized hosts from connecting to the network.**

To enforce authorized access, the solution maintains an authorization database of IP-MAC mappings and responds to ARP broadcasts from unauthorized hosts with the MAC of a captive portal as the destination.

Which of the following is most likely used for the solution to redirect the unauthorized hosts to the captive portal?

A. Spoofing
B. Layering
C. Encapsulation
D. Compromise recording

☞ Answer to QOTD: 20200717

179. **Your company is constructing a new building with a structured cable system topology per the standard**

EIA/TIA 568. As a network engineer, you are designing an 802.3 network with hundreds of nodes.

Which of the following is the best strategy to mitigate the threat of network sniffing and denial of services?

A. Manage the network with security domains
B. Separate the network into broadcast domains
C. Split the network into collision domains
D. Organize the network into DNS domains

☞ Answer to QOTD: 20200320

180. **The man-in-the-middle attack intercepts, relays, and possibly alters the communication between two systems.**

Which of the following incorporates encryption to mitigate the threat of a middle man?

A. DSSS (Direct Sequence Spread Spectrum)
B. ARP (Address Resolution Protocol)
C. TCP (Transmission Control Protocol)
D. DNS (Domain Name System)

☞ Answer to QOTD: 20200505

181. **The E-commerce web site of your company is suffering a DoS attack by flooding Christmas tree packets on Christmas day when the incident response team members are going home for a family reunion.**

Which of the following best describes this attack?

A. A Christmas tree packet is an IP packet with flags FIN, PSH, and URG turned on
B. A Christmas tree attack comes from the logic bomb on zombies triggered on Christmas day
C. A Christmas tree attack is one type of cryptoanalysis

attack
D. A Christmas tree packet affects both routers and the endpoints

☞ Answer to QOTD: 20191225

182. **A threat event can be elaborated in terms of tactics, techniques, and procedures (TTP). An attacker initiates a DDoS (Distributed Denial-of-Service) attack from zombies in a botnet through DNS services to attack a victim.**

Which of the following techniques is least likely used in this attack?

A. Blackholing
B. Reflection
C. Flooding
D. Amplification

☞ Answer to QOTD: 20200506

183. **A threat event can be elaborated in terms of tactics, techniques, and procedures (TTP).**

An attacker initiates a DDoS (Distributed Denial-of-Service) attack from zombies in a botnet through DNS services to attack a victim.

Which of the following techniques best describes sending DNS requests with a spoofed source address from zombies to generate a large volume of DNS responses to the victim?

A. Amplification
B. Flooding
C. Reflection
D. Smurfing

☞ Answer to QOTD: 20200507

184. **Your company sells toys online worldwide, which is supported by a three-tiered E-Commerce web-based system.**

You observed an egress pattern of traffic from the EC system to a remote host. You suspect it is a covert timing channel.

Which of the following is the least concern in terms of the covert channel?

A. HTTP
B. TCP
C. ICMP
D. ARP

☞ Answer to QOTD: 20200516

185. **You are participating in a project designing and implementing the company network for a startup.**

As a security professional, which of the following is the least concern in terms of the Network layer?

A. Teardrop attack
B. Smurf attack
C. Route poisoning
D. Fraggle attack

☞ Answer to QOTD: 20200605

186. **Your company is a well-known cloud services provider. You received one day, tons of complaints from customers about a sudden drop in network performance for hours.**

An incident investigation is initiated and finally concluded that misconfigured routing between autonomous systems from a peer service provider is the root cause.

Which of the following is the most probable threat scenario?

A. The peer service provider causes a routing loop between neighbors without a metric that counts to infinity.
B. The peer service provider sends wrong routing entries with non-standard compliant interior gateway protocols.
C. The peer service provider redirects the traffic to its networks intentionally or unintentionally.
D. The peer service provider overloads the voice and data traffic by Signaling System No. 7 (SS7).

☞ Answer to QOTD: 20200504

DOMAIN 5: IDENTITY AND ACCESS MANAGEMENT (IAM)

ENROLLMENT AND IDENTITY PROOFING

187. **You are considering assurance levels of digital identity and digital authentication, which of the following avoids a false claimant using a credential that is not rightfully theirs?**

A. Identity Assurance Levels (IAL)
B. Authenticator Assurance Levels (AAL)
C. Federation Assurance Levels (FAL)
D. Evaluation Assurance Levels (EAL)

☞ Answer to QOTD: 20191205

188. **A new business partner is applying for a VPN account in your company to work remotely. However, the password settings for partners are the same as those for employees.**

As a security professional, you consider the risk is higher for remote partners than inside workers, and the system administrator should provision password settings at a stricter and fine-grained level.

A system administrator created a new account, generated a password randomly, and text him a URL in his mobile phone to activate the account.

Which of the following should be considered most in terms of the provisioning process?

A. Identity Assurance Levels (IAL)
B. Authenticator Assurance Levels (AAL)
C. Federation Assurance Levels (FAL)
D. Evaluation Assurance Levels (EAL)

☞ Answer to QOTD: 20191206

189. **Your company sells toys online and ships globally. The cryptographic implementation of the shopping website follows FIPS (Federal Information Processing Standards).**

The customer service representatives (CSR) report a serious workload issue that customer complaints flock in from all service channels about the inconvenience of the website password reset procedure.

If retrieving passwords is technically impossible, which of the following cryptographic algorithms is most likely to cause this problem?

A. DES (Data Encryption Algorithm)
B. SHA (Secure Hash Algorithms)
C. MD5 (Message Digest)
D. Advanced Encryption Standard (AES)

☞ Answer to QOTD: 20200228

190. **Your company sells toys online and ships globally. The online shopping website would send the original password back to the cell phone if the customer forgot the password.**

Which of the following is the best cryptographic algorithm used to protect the password at rest?

A. 3DES (Triple Data Encryption Algorithm)
B. Salted SHA (Secure Hash Algorithms)
C. HMAC (Hashed Message Authentication Code)
D. Hardware token

☞ Answer to QOTD: 20200223

191. **Your company sells toys online and ships globally. The shopping website employs a weak password**

policy and stores the customer's password as an MD5 hash in the database.

After conducting a password assessment, the report discloses that many customers use the notorious naive password '0000'.

Which of the following can best address the vulnerability to mitigate rainbow table attacks?

A. Replace MD5 with SHA2
B. Implement cell-level encryption in the database
C. Prepend or append strings before computing hashes
D. Employ initialization vector to increase entropy

☞ Answer to QOTD: 20200226

192. **You are conducting pentesting and have exploited a vulnerability to gain access to the file, /etc/shadow, in which one line reads as follows:**

root:1vb1tLY1q$6jf7S0s1/qsCHOGJLrDb.1:18009:0:120:7:14::

Which of the following is the most feasible to crack the line?

A. Resolve by searching open-source intelligence
B. Try every possible combination
C. Employ a text file of the MD5 hash values
D. Download a table of pre-computed values in SHA

☞ Answer to QOTD: 20200715

193. **Your company sells toys online and ships globally. As a security professional, you are planning for a security assessment. As the password attack is one of the most common attacks, for example, brute force attack, dictionary attack, rainbow table attack, and so forth,**

an external security team will be employed to inspect weak passwords.

For experienced, ethical hackers, which of the following passwords most likely takes the highest cryptanalysis work factor?

A. 0000
B. uTqD3S^#
C. !@#$%^&*
D. 4a7d1ed414474e4033ac29ccb8653d9b

☞ Answer to QOTD: 20200229

PROVISIONING AND DEPROVISIONING

195. **Jack is a new employee. As the account administrator, you are provisioning a new user account and its privileges for Jack based on a template user account.**

Which of the following is least related to the provisioning process?

A. Service Provisioning Markup Language (SPML)
B. Take-Grant Model
C. Access Control Matrix
D. Security labeling

☞ Answer to QOTD: 20200311

196. **Your company implemented a variety of information systems that host their user accounts, and an LDAP-compliant directory maintained by the Human Resource department.**

The development team is developing a solution that streamlines the HR processes to create and synchronize new employee accounts and assign privileges across systems.

As a security professional, which of the following will you recommend the most?

A. Federated Identity
B. XACML (eXtensible Access Control Markup Language)
C. SPML (Service Provisioning Markup Language)
D. IDaaS (Identity as a Service)

☞ Answer to QOTD: 20191211

AUTHENTICATION

197. **Your company usually holds meetings with partners, suppliers, or consultants in the meeting rooms on the 1st floor, a public workspace isolated from the internal network.**

However, employees need to connect their devices to the internal network for business purposes. You are evaluating VPN solutions that use multi-factor authentication (MFA) to address this issue.

Which of the following authentication mechanisms best meets your requirement?

A. EAP-TLS
B. ODIC (OpenID Connect)
C. Smart card plus cognitive password
D. SAML (Security Assertion Markup Language)

☞ Answer to QOTD: 20190930

198. **Your company decides to start the business of selling toys online and shipping globally. The E-Commerce system that supports the new business will be developed in-house.**

In a requirement workshop, the representative of the customer support department suggests when a user logged in with the wrong password, the system shall display a message, "Invalid password. please login again." It is because users are frequently calling for customer support to reset the password but insist they didn't type the password wrong.

As a security professional, which of the following should you suggest first?

A. Use a semantic passphrase
B. Automate the reset password process
C. Revise the message to guide the reattempts of login
D. Lower the requirement of password length

☞ Answer to QOTD: 20191010

199. **Your company is selling toys online and shipping globally.**

When signing in to the web site, a customer, Jack, forgot his password. He clicked the "Forgot password?" button to reset his password and received a password notification email in 2 minutes that provided his old password for him to sign in.

Jack called the customer service to complain about the insecure web system because of receiving the password notification email.

As a security professional, which of the following is the best suggestion?

A. Implement a self-service portal to reset password
B. Accelerate the delivery speed of password notification emails
C. Employ a one-way function to handle passwords and concatenated random strings
D. Use AES256 to encrypt passwords with salts

☞ Answer to QOTD: 20191023

200. **Your organization is developing a Transportation Management System (TMS) that processes two types of data: air and ground transportation data.**

Confidentiality and cost-effectiveness are the most concern of your organization, and biometric

authentication belongs to the security control baseline for high-impact systems.

After the business and privacy impact analysis, incidents such as data breach, unauthorized change, and loss of access to any transportation data will cause a low impact on your organization.

However, unauthorized alteration to air transportation data renders a moderate impact. It is about time to determine baseline security controls based on the system impact level.

Which of the following is the best decision according to the impact analysis?

A. Implement a fingerprint-based authentication system
B. Implement a hardware token authentication system
C. Implement an authentication system based on something you know
D. Implement a two-factor authentication system

☞ Answer to QOTD: 20200213

201. **Your company decides to start the business of selling toys online and shipping globally. A team in-house is in charge of developing a web-based E-Commerce system that supports the new business. The team is evaluating the authentication solution.**

Which of the following is the least feasible?

A. Use the 'Basic' HTTP authentication encoded with Base64 but not encrypted
B. Use HTTP Digest access authentication that relies on browser implementation
C. Implement Kerberos to protect passwords and facilitate single sign-on (SSO)

D. Develop a proprietary mechanism by sending an HTML form via HTTP POST in clear text

☞ Answer to QOTD: 20191213

202. **Your company requires that passwords cannot be cracked in one year with a brute force attack. You are implementing a password policy by specifying valid characters, as shown in the regular expression, /[a-zA-Z0-9!$]/.**

If it takes 4 hours to crack passwords with a length of 7 characters, what is the minimum password length to meet your company's password requirement?

A. Seven characters
B. Eight characters
C. Nine characters
D. Ten characters

☞ Answer to QOTD: 20191210

EAP AND 802.1X

204. **You are implementing remote access solutions to support employees traveling on business. They will connect mobile phones or laptops to corporate networks, on the road, or in the hotel, via the unprotected public network. Which of the following is least likely used?**

A. 802.1X
B. eXtensible Access Control Markup Language
C. IPsec VPN with tunnel mode
D. RADIUS

☞ Answer to QOTD: 20190920

205. **You are working for a high-tech blue-chip company in which research and development data is highly protected. All wired network access ports are disabled by default except those controlled for production or work purposes by 802.1X. The current Acceptable Usage Policy (AUP) states that any form of intranet wireless access is prohibited without exception. In a product engineering meeting, the vice president of R&D is requesting confined wireless access in the meeting room for convenience and efficiency. As a security professional, which of the following is the best way to deal with this situation?**

A. Just note it down and file a case
B. Apply 802.1X to wireless access with WPA2 and use VPN connection
C. Implement a faraday cage and white noise to confine radiation in the meeting room
D. Revise the Acceptable Usage Policy (AUP)

☞ Answer to QOTD: 20190912

206. **There are many visitors and employees holding meetings in the meeting rooms in your company. Oftentimes, they need to plug their laptops to the Ethernet ports in the meeting room or connect to the wireless access points to get access to the internet for business purposes. You are evaluating the Network Access Protection (NAP) solutions.**

Which of the following is the least feasible?

A. Maintain a white list for MAC filtering
B. Implement 802.1X or EAP over LAN
C. Enable DHCP snooping
D. Use VLAN to isolate traffic

☞ Answer to QOTD: 20190929

KERBEROS

207. **You are developing an in-house application with an authentication requirement that user passwords shall not be transmitted on the network.**

Which of the following is the best solution for clients to authenticate to the server?

A. Clients encrypt credentials using the server's public key.
B. The server sends a nonce encrypted by the client's public key.
C. Clients negotiate a dynamic key with the server through Diffie-Hellman.
D. The server sends a TGT encrypted by its secret key after receiving the client's ID.

☞ Answer to QOTD: 20200807

208. **In the Kerberos network authentication system, a client initiates authentication requests to the authentication service (AS) to obtain authentication credentials for a given server.**

Which of the following is not true?

A. The AS is subject to the chosen-ciphertext attack.
B. The client sends its own identity to the AS in cleartext when logging in.
C. The AS doesn't know whether the client sends a genuine identity or not.
D. The client doesn't send its password or secret key to the AS when logging in.

☞ Answer to QOTD: 20200805

209. **In the Kerberos network authentication system, clients, the KDC, and application servers are the well-**

known three-headed architectural components.

Which of the following best describes the operations of Kerberos?

A. The KDC manages all the keys and is resistant to denial-of-service attacks.
B. Clients on the network interact with the KDC and servers asynchronously.
C. Realms must be organized hierarchically to support cross-realm authentication.
D. Initial ticket requests from clients are handled by the authentication service (AS).

☞ Answer to QOTD: 20200804

OTP TOKEN

210. **A bank is evaluating two models of one-time password tokens for multi-factor authentication. Both models have a button, an LCD, volatile memory, and a battery, but no keypad. Model A uses a non-replaceable battery, while the battery of Model B must be replaced in three minutes if the low battery.**

    Which of the following token types is most likely implemented by Model A?

    A. Static password token
    B. Synchronous dynamic password token
    C. Asynchronous password token
    D. Challenge-response token

    ☞ Answer to QOTD: 20200703

211. **A bank is evaluating two models of one-time password tokens for multi-factor authentication. Both models have a button, an LCD, volatile memory, and a battery, but no keypad. Model A uses a non-replaceable battery, while the battery of Model B must be replaced in three minutes if the low battery.**

    Which of the following token types is most likely implemented by Model B?

    A. Static password token
    B. Synchronous dynamic password token
    C. Asynchronous password token
    D. Challenge-response token

    ☞ Answer to QOTD: 20200704

212. **You are evaluating the one-time password (OTP) solutions, and a vendor proposed two models of OTP**

tokens. One solution is synchronous; the other is asynchronous.

Which of the following is the primary cryptographic algorithm used in the synchronous solution to generate passwords?

A. Lucifer
B. Rijndael
C. HMAC
D. Clock timer

☞ Answer to QOTD: 20200716

BIOMETRIC

213. **Your company decides to sell toys online and ships globally. The target customers are house-hold consumers. An in-house team is responsible for developing the online shopping website. To maximize security assurance and market share, which of the following is the best authentication solution?**

A. Iris
B. Fingerprint
C. Password
D. Retina

☞ Answer to QOTD: 20200309

214. **Your company is evaluating a new biometric access control system. Requirements for ease of use and user acceptance precede the level of security. The budget is not a concern. However, the error rate shall not exceed 3 times per day. There are 500 employees in the office building; each of them will go in and out 10 times on average every day. Three vendors submitted proposals as follows:**
- Vendor A: Fingerprint, CER: 0.05%
- Vendor B: Iris, CER: 0.02%
- Vendor C: Retina, CER: 0.01%
As a security professional, which of the following solution will you suggest?

A. Vendor A
B. Vendor B
C. Vendor C
D. Any of them

☞ Answer to QOTD: 20191208

215. **Your company implemented a new fingerprint access control system. It seemingly does not work properly as you and many employees are sometimes rejected out of the door, and the recognition speed is annoying.**

Which of the following is the best to address this issue?

A. Increase the False Rejection Rate (FRR)
B. Decrease the False Acceptance Rate (FAR)
C. Implement one-to-one authentication
D. Lower Equal Error Rate (EER)

☞ Answer to QOTD: 20191207

SINGLE SIGN-ON (SSO)

216. **Your company decides to start the business of selling toys online and shipping globally. The E-Commerce system that supports the new business will be developed in-house. The client is executed in modern web browsers. The development team is evaluating the single sign-on (SSO) solution.**

    Which of the following least likely meets the requirement of SSO?

    A. OAuth
    B. OIDC (OpenID Connect)
    C. SAML (Security Assertion Markup Language)
    D. XACML (eXtensible Access Control Markup Language)

    ☞ Answer to QOTD: 20191003

217. **Which of the following statement about single sign-on (SSO) is not true?**

    A. SSO enables users to log in once and gain access to resources across systems
    B. Multiple user accounts registered across systems can achieve SSO
    C. SSO may involve multiple logins across systems
    D. SSO is achieved by maintaining only one account trusted across systems for each user

    ☞ Answer to QOTD: 20191203

218. **Which of the following statements about single sign-on (SSO) is not true?**

    A. A user can sign on a system once and access other systems without re-authentication
    B. An SSO user account causes more serious impact then

non-SSO if breached
C. Systems require federation protocols to support SSO
D. A user can create multiple user accounts across systems that support SSO

☞ Answer to QOTD: 20200402

219. **Single sign-on enables users to gain access to multiple information system resources through federated identity.**

All of the following support single sign-on (SSO) except which one?

A. Credential Management Systems
B. Kerberos
C. Scripted access or logon scripts
D. Identity Federation

☞ Answer to QOTD: 20191204

IDENTITY FEDERATION

220. **Which of the following is the best authentication standard or protocol for the extranet integration based on SOAP?**

A. LDAP
B. OIDC
C. XACML
D. SAML

☞ Answer to QOTD: 20200403

221. **Your company implemented Federated Identity Management (FIM) based on SAML to support Single Sign-On (SSO).**

Which of the following is not true?

A. A user may have an identity in each domain and multiple identities across domains.
B. A federated identity is a pseudonym shared between domains to hide a user's identity.
C. A relying party authorizes access requests based on assertions expressed in XACML.
D. SSO relies on the service provider's (SP) trust in the Identity Provider (IdP).

☞ Answer to QOTD: 20200806

222. **SAML refers to Security Assertion Markup Language. Which of the following statements about "assertion" is not true?**

A. It is a package of information produced by the relying party
B. It describes an act of authentication performed on a subject

C. It contains attribute information about the subject
D. It may have authorization data for the subject to access a specified resource

☞ Answer to QOTD: 20200408

223. **Your company sells toys online and ships globally. After a customer is authenticated, the client browser receives the following HTTP response:**

```
HTTP/1.1 200 OK
Content-Type: application/json
{
 "sub": "VIP202003010001",
 "name": "Alice",
 "email": "alice@effectivecissp.com",
 "picture": "http://effectivecissp.com/i/alice.jpg "
}
```

Which of the following best describes the protocol or standard the website supports?

A. Federated Identity Management (FIM)
B. Security Assertion Markup Language (SAML)
C. OIDC (OpenID Connect)
D. SSO (Single Sign-On)

☞ Answer to QOTD: 20200302

SESSION MANAGEMENT

224. **A session can be established based on connection-oriented or connectionless transport and other underlying services. Which of the following communications least requires a session?**

A. An authenticated browser sending HTTP requests without the Keep-Alive header
B. The zone transfer between the primary and secondary DNS servers
C. Server cluster members periodically sending heartbeat
D. A user listening to his or her subscribed online music

☞ Answer to QOTD: 20200312

225. **Your company sells toys online worldwide, which is supported by a web-based E-Commerce system. The EC system issues an access token, which is renewed on a rolling basis, for subsequent access authorization after a user is validated.**

You disabled a user account after confirming an active session is established using the breached user account. However, the access token and the user session are still active, and resources are accessible. Which of the following is the best solution to solve this problem?

A. Implement complete mediation
B. Impose a higher degree of race condition
C. Conduct Time-of-Check after Time-of-Use
D. Apply need-to-know and least privilege principles

☞ Answer to QOTD: 20200519

226. **A session begins with an authentication event and refers to all the subject's activities that take place**

during its establishment, maintenance, and release.

Web sessions are typically maintained through a session identifier transmitted back and forth between the client and the webserver.

Which of the following is not an option to manage the session?

A. HTTP cookies
B. HTTP requests
C. HTTP status code
D. HTML hidden inputs

☞ Answer to QOTD: 20200818

AUTHORIZATION

227. **Which of the following least contributes to access control on the need-to-know basis?**

A. An object with non-hierarchical label
B. A subject's capability table
C. A subject's security clearance
D. A compartmented object

☞ Answer to QOTD: 20200701

228. **Your company sells toys online worldwide. Supporting information systems implements DAC, RBAC, ABAC, and RuBAC to mediate access control.**

The sales manager, as a data owner, is considering authorizing Alice access to the customer profiles.

Which of the following is the least concern?

A. Need-to-know
B. Least privilege
C. Conflict of interest
D. Security clearance

☞ Answer to QOTD: 20200510

229. **The development team of your company is implementing a web-based multi-tiered Procurement Management System.**

Purchase orders shall be approved before issuance by different management levels based on a variety of criteria, e.g., Order Amount, Supplier, or Product Category.

As criteria are subject to change, the development team decides not to hard code the approval logics and

policies but implements a user interface for the procurement manager to manage them.

The web server delegates the authorization decision of requests from web clients to a remote authorization server that will refer to the approval policies managed by the procurement manager.

If the authorization mechanism is based on XACML, which of the following roles is the web server?

A. Policy Enforcement Point (PEP)
B. Policy Decision Point (PDP)
C. Policy Administration Point (PAP)
D. Policy Information Point (PIP)

☞ Answer to QOTD: 20191212

230. **An offboarding sales representative downloaded customer profiles owned by the head of the sales department from the file server onto a USB dongle on the day he left and sold it online.**

This data breach occurred because of the miscommunication between the HR and IT departments. The HR department didn't notify the IT department to disable the user accounts and revoke the privileges of the unhappy employee in time.

Which of the following best contributes to the solution that can prevent the data breach?

A. LDAP
B. XACML
C. SAML
D. SPML

☞ Answer to QOTD: 20200706

231. **Which of the following provides the most flexible access control?**

A. A subject asserting unmarried
B. A subject with the Top Secret clearance
C. A subject with need-to-know
D. A subject assigned to the Admin role

☞ Answer to QOTD: 20190514

232. **Firewalls are one of your company's product lines. The engineering team is designing a new proxy firewall that shall authenticate users to authorize internet access.**

Which of the following is the best to control internet access?

A. Non-discretionary Access Control
B. Discretionary Access Control
C. Rule-based Access Control
D. Role-based Access Control

☞ Answer to QOTD: 20191115

233. **Your company decides to start the business of selling toys online and shipping globally. The E-Commerce system that supports the new business will be developed in-house.**

In a requirement workshop, a participant proposed that discounted products in promotion campaigns shall be purchased by those customers who meet the criteria specified by marketing staff, e.g., customer's identity, gender, role, city, income, login time, device type, etc. The development team considers the authorization rules of purchase are too complicated.

As a security professional, which of the following will you best recommend to address the requirement?

A. Lattice-based access control
B. Role-based access control
C. Attribute-based access control
D. Rule-based access control

☞ Answer to QOTD: 20191012

ACCOUNTABILITY

235. **You are the development team leader and recently found your nightly build failed from time to time.**

Eve was a disgruntled developer in your team and quit last month. She is responsible for part of the solution and is not authorized to integrate the solution.

She installed a program running under the local system privilege to delete, on Monday midnights, some source code in the local code repository pushed to the central code repository to be integrated.

You decide to conclude that Eve is accountable for the failures of the nightly builds.

Which of the following is the least important?

A. Authentication
B. Authorization
C. Auditing
D. Non-repudiation

☞ Answer to QOTD: 20200821

236. **Your company decides to start the business of selling toys online and shipping globally. A team in-house is in charge of developing an E-Commerce system that supports the new business. You suspect a former developer deleted some crucial files before leaving the company.**

Which of the following least helps to blame the malicious behavior on him?

A. Implement reliable authentication mechanism
B. Grant permissions and rights based on duties
C. Maintain a non-reputable log

D. Correlate and review the logs in terms of a specific subject or theme

☞ Answer to QOTD: 20191125

PHYSICAL ACCESS CONTROL

237. **In physical security, the employment of barriers with the capacity to delay the progress of an intruder is one of the security designs of the Defense-in-Depth (DiD) strategy.**

To validate the effectiveness of the design, which of the following should be conducted first?

A. Target hardening
B. Universal element conceptual mapping
C. Critical path analysis
D. Fire drill to protect life

☞ Answer to QOTD: 20200509

238. **You are conducting user acceptance testing against the fingerprint-based physical access control to the computer room. System administrators and engineers report that they are often blocked outside the door.**

Which of the following is the most feasible solution to solve this problem?

A. Lower the error rate of the CER
B. Lower the slope of the FRR curve to reduce Type I error
C. Lower the slope of the FAR curve to reduce Type II error
D. Ask the vendor to replace the fingerprint reader with a new one having lower EER

☞ Answer to QOTD: 20200808

239. **You are implementing a mantrap to control the access to a highly regulated lab for the research of the COVID-19 vaccine to prevent piggybacking and tailgating. It**

uses two-pass authentication: an ID card for the external door and facial recognition for the other.

Which of the following should be the concern at priority and addressed first?

A. Refer to the product manual for the mean time to failure (MTTF)
B. Refer to the product manual for the default failure mode configuration
C. Refer to the product manual for low false rejection rate (FRR) configuration
D. Refer to the product manual for low false acceptance rate (FAR) configuration

☞ Answer to QOTD: 20200809

240. **Your company implements a physical access control system (PACS) that authenticates employees through ID credentials of contactless smart cards. As a security professional, you are conducting threat modeling.**

Which of the following threats least entails a legitimate ID card in terms of personal identification verification?

A. Sniffing
B. Skimming
C. Counterfeiting
D. Social engineering

☞ Answer to QOTD: 20200811

241. **Your company is evaluating a physical access control system (PACS) solution. As a security professional, which of the following is the weakest authentication mechanism that you won't recommend?**

A. ID card using the default PIN code
B. Unattended iris scanning with a high FAR
C. Fingerprint scanning with the default threshold
D. Security guards conducting visual authentication

☞ Answer to QOTD: 20200812

DOMAIN 6: SECURITY ASSESSMENT AND TESTING

SECURITY ASSESSMENT

242. **Which of the following best describes the process of evaluating the effectiveness of security controls through interviewing, examination, and testing?**

A. Risk assessment
B. Vulnerability assessment
C. Risk evaluation
D. Security assessment

☞ Answer to QOTD: 20200420

243. **You are the CISO working for a direct bank based in Taiwan that relies entirely on internet banking. You want to evaluate if security controls are implemented correctly, operating as intended, and producing the desired outcome.**

Which of the following should you conduct?

A. Risk assessment
B. Third-party audit
C. Business impact analysis
D. Security control assessment

☞ Answer to QOTD: 20200119

244. **Your organization conducts full backup on Sundays and incremental backup on weekdays and Saturdays, all at midnight and supported by a highly automated tape library and offsite tape vaulting. An internal auditor asked the backup operator to restore tapes to a spare server to verify the effectiveness of the backup.**

Which of the following assessment methods does the internal auditor employ?

A. Simulation
B. Interviewing
C. Testing
D. Examination

☞ Answer to QOTD: 20200219

245. **As a CISO, you issue a policy that mandates every employee shall be aware of social engineering attacks. A supporting standard is then developed that requires everyone shall accept at least three or more hours of awareness training each year.**

Which of the following activities is the best upcoming activity conducted to enforce the policy?

A. Penetration testing
B. Security assessment
C. Vulnerability assessment
D. Risk assessment

☞ Answer to QOTD: 20200528

246. **You are planning for a security assessment project to ensure compliance and security. Vulnerability assessment of information systems and the capability of incident response shall be conducted.**

Which of the following approaches or methodologies best meets your requirements?

A. Threat Modeling with STRIDE
B. NIST RMF (Risk Management Framework)
C. Open Source Security Testing Methodology Manual (OSSTMM)
D. Risk assessment

☞ Answer to QOTD: 20200429

PENETRATION TESTING

247. **You are the CISO working for a direct bank based in Taiwan that relies entirely on internet banking. The security assessment team has completed penetration testing as part of the risk assessment, which identified some significant vulnerabilities. You are reviewing the assessment report.**

Which of the following will you expect the most in the report?

A. Prioritized vulnerabilities based on CVSS
B. Business impact analysis in terms of monetary value
C. Business case
D. Threat scenario analysis

☞ Answer to QOTD: 20200104

248. **You have engaged in a double-blind pentest contract and get started to conduct testing. To effectively assess vulnerabilities and keep the testing in secret, which of the following should be conducted first?**

A. Enumerate services on hosts to discover potential attack vectors
B. Conduct passive testing against the target
C. Exploit vulnerabilities by sending passive payloads
D. Cloak a port scan with decoys to hide your IP address

☞ Answer to QOTD: 20200427

249. **You have engaged in a double-blind pentest contract and get started to conduct testing. After searching the client's WHOIS DNS data and job vacancies posted on job boards, you decide to proceed to the next stage.**

Which of the following activities least likely follows what you have completed?

A. Lookup the DNS MX records
B. Masquerade as a job applicant
C. Conduct OSINT (Open-source intelligence)
D. Cloak a port scan with decoys to hide your IP address

☞ Answer to QOTD: 20200428

250. **You hired an external penetration test team to assess your company's web sites. After receiving the penetration test report, which of the following should you conduct first?**

A. Apply patches to mitigate vulnerabilities
B. Prepare a follow-up report for management review and decision
C. Take corrective actions for correction and improvement
D. Improve the performance and security of the web sites continuously

☞ Answer to QOTD: 20200430

251. **Your company outsourced the penetration testing project to an external party conducting ethical hacking. The project, as a black box, is conducted in secret.**

Which of the following is least likely to entail penetration testing?

A. Patch management
B. Risk assessment
C. Security control assessment
D. Threat modeling

☞ Answer to QOTD: 20200511

252. **Your company sells toys online worldwide. A web-based E-Commerce system developed in-house and deployed to a public cloud supports the business. As a security professional, you suggest that penetration testing should be conducted.**

Which of the following is your most concern?

A. The decision of employment of internal or external penetration test team
B. The capability and experience of the penetration test team
C. The procedure that the penetration test team asks for permission to conduct penetration testing
D. The escalation path to the senior management if testing takes down the system

☞ Answer to QOTD: 20200529

253. **A penetration testing team is conducting reconnaissance. Which of the following is the most likely output?**

A. A list of services running on a host
B. A list of vulnerabilities identified by CVE
C. A list of network hosts
D. A list of unpatched services

☞ Answer to QOTD: 20200607

254. **After penetration testing, a vulnerability on a web server is identified and confirmed. Which of the following actions should be taken first?**

A. Apply patches in time
B. Conduct change management
C. Conduct risk assessment
D. Conduct configuration management

☞ Answer to QOTD: 20200404

SECURITY AUDIT

255. **You are working for a company as the CISO. Your company decided to go for the ISO 27001 certification. After six months of preparation, the external audit by a certain certification body is scheduled for next Monday. If your company passes the audit, it will receive the ISO 27001 certificate.**

Which of the following is the least common activity conducted by the external auditors?

A. Invite senior management for meeting
B. Consult subject matter experts
C. Conduct penetration testing to validate the security controls
D. Ask for documents before on-site auditing

☞ Answer to QOTD: 20190919

256. **You are the CISO working for a direct bank based in Taiwan that relies entirely on internet banking. Your bank is implementing an information security management system (ISMS) compliant with ISO 27001 and undergoing a certification audit. An external auditor is interviewing with you. In which of the following issues is the auditor least likely to be interested during the interview?**

A. Are the roles and responsibilities assigned and communicated
B. Is the information security policy available as documented information
C. Are there any needs for changes to the ISMS
D. Is risk assessment conducted before business impact analysis

☞ Answer to QOTD: 20200109

257. **You are the CISO working for a US-based startup company offering customer relationship management (CRM) solutions as SaaS. Your company is about to bid for a big deal that requires vendors to demonstrate assurance of security and privacy based on the AICPA's Trust Services Criteria (TSCs). The bidding process will be closed in one month. Your company has just received its first certification, ISO 27001. To win the bid, which of the following will you best recommend?**

A. PCI-DSS
B. SOC 2 Type I
C. SOC 2 Type II
D. SOC 3

☞ Answer to QOTD: 20200110

258. **You are the CISO working for a direct bank based in Taiwan that relies entirely on internet banking. You are reviewing the performance of security operations.**

Which of the following is most likely out of the review scope?

A. Development progress of the business continuity plan
B. Walkthrough result of the disaster recovery plan
C. The efficiency of the incident response
D. The validity of backup data

☞ Answer to QOTD: 20200114

259. **You are the CISO working for a direct bank based in Taiwan that relies entirely on internet banking. You developed an information security policy and put it into effect.**

Which of the following is the most effective for you to enforce its compliance?

A. Provide more training to improve awareness and skill levels
B. Conduct frequent audits to improve continuously
C. Develop standards, procedures, and guidelines to support the policy
D. Collaborate with the audit department

☞ Answer to QOTD: 20200115

260. **You are the CISO working for a direct bank based in Taiwan that relies entirely on internet banking. You are collaborating with auditors to facilitate auditing activities to ensure compliance with information security policy.**

Which of the following is least commonly adopted?

A. Employing the Delphi method
B. Interviewing with senior management
C. Reviewing data backup policy
D. Sending questionnaires to the target group

☞ Answer to QOTD: 20200116

261. **As a CISSP working for a direct bank based in Taiwan that relies entirely on internet banking that involves credit card business, you are reviewing compliance requirements.**

Which of the following is least related to the compliance issue?

A. Customer's contracts
B. Foreign laws
C. (ISC)² Code of Ethics
D. Due diligence in mergers and acquisitions

☞ Answer to QOTD: 20200124

262. **Your company is a well-known cloud services provider. As a security professional, you designed a set of security controls to ensure the provisioning of trust services. To increase customer's confidence and provide security assurance, you are seeking attestation of the suitability of your design from one of the big four accounting firms.**

Which of the following is the best attestation engagement?

A. Type 1 SOC 1
B. Type 2 SOC 3
C. Type 1 SOC 2
D. Type 2 SOC 2

☞ Answer to QOTD: 20200502

263. **Your company sells toys online across the world. A PaaS supports the online EC system that accepts credit cards. The staff and management conduct periodic, proactive reviews of controls to assure stakeholders that the internal control system of the organization is reliable.**

Which of the following is the best description of this management practice?

A. SOC-2 audit
B. PCI-DSS audit
C. ISO 27001 audit
D. Self-assessment

☞ Answer to QOTD: 20200813

264. **You work for a US-based public company that sells toys all over the world. A PaaS supports the online EC system that accepts credit cards.**

As an internal auditor, which of the following least concerns you in terms of compliance?

A. PCI-DSS
B. Baselines
C. Sarbanes-Oxley Act (SOX)
D. Information security policy

☞ Answer to QOTD: 20200814

DOMAIN 7: SECURITY OPERATIONS

BUSINESS CONTINUITY

265. **You are a member of the steering committee for the program of the business continuity management system and in a meeting with the agenda of business impact analysis to determine the Maximum Tolerable Period Downtimes (MTPDs) and recovery time objectives (RTOs). All of the following should have been done prior to the meeting except what?**

A. Plan for actions to address risks to the effectiveness of the management system
B. Establish the business continuity policy
C. Conduct risk assessment in terms of business activities
D. Understand the organization's context and interested parties

☞ Answer to QOTD: 20191127

266. **As the newly hired CISO for a global company selling toys all over the world, you are reviewing the company's mission statement and organizational structure and processes, identifying applicable legal and regulatory requirements, and interviewing stakeholders to implement the business continuity management system (BCMS).**

Which of the following is the most likely activity you will do next?

A. Conduct business impact analysis
B. Determine the scope
C. Assess risk
D. Develop the business continuity plan

☞ Answer to QOTD: 20200629

267. **Your company initiates a business continuity program to support the continuous delivery of products and services. You're in charge of the reliability and availability of the power system, including UPS and the power generator. Which of the following is the least concern for you?**

A. The default failure mode configuration
B. The mean time to repair (MTTR)
C. The mean time to failure (MTTF)
D. Service level agreement (SLA)

☞ Answer to QOTD: 20200810

268. **Which of the following is not the output of business impact analysis?**

A. A list of identified risks or threats
B. Critical process or prioritized activities
C. Capacity of operations
D. Recovery Time Objective (RTO)

☞ Answer to QOTD: 20200407

269. **You are preparing for Information System Contingency Plan (ISCP) and considering solutions of alternate sites. Which of the following is not one of the objectives that directly drive your planning work in terms of information systems?**

A. Maximum Tolerable Downtime (MTD)
B. Service Delivery Objective (SDO)
C. Recovery Point Objective (RPO)
D. Recovery Time Objective (RTO)

☞ Answer to QOTD: 20200406

270. **Your company, with regional offices across the country, sells toys online and ships globally. As the WHO announced that COVID-19 goes pandemic, you are responsible for responding to this crisis and evaluating the working-at-home solution.**

As a CISO, which of the following should be the highest priority?

A. Enforce remote access control
B. Review asset inventory, e.g., VPN licenses
C. Publish recommendations for cleaning, disinfection, and healthcare
D. Test the disaster recovery plan (DRP)

☞ Answer to QOTD: 20200314

271. **You are a member of the program of business continuity management system (BCMS) and sitting in a meeting with the agenda of determining the scope of the BCMS.**

Which of the following activity is least likely to be conducted?

A. SWOT analysis
B. Cost-benefit analysis
C. Stakeholder or interested party analysis
D. Documentation

☞ Answer to QOTD: 20191128

272. **You are a member of the program of business continuity management system (BCMS) and sitting in a meeting. After the discussion, there are some findings from your company.**

A plant in Taiwan manufactures sports towels and markets around the world; another plant in Vietnam

primarily makes shoes for a worldwide label that mandates your company shall fulfill its purchase orders without interruption.

Based on the findings, which of the following activity should be conducted first?

A. Conduct business impact analysis (BIA)
B. Determine the scope
C. Assess risk in terms of products and services and related resources
D. Identify strategies and solutions

☞ Answer to QOTD: 20191129

273. **As a CISO, you intend to establish a business continuity management system (BCMS) compliant with the ISO 22301 standard. You are considering the scope of the BCMS.**

Which of the following least affects your decision of the scope?

A. Business impact analysis
B. Customer's needs
C. Organizational structure
D. Employee's attitude

☞ Answer to QOTD: 20191215

274. **In a risk management workshop, a team member identified a risk related to the uninterruptible power supply (UPS). If the UPS batteries are not replaced regularly, the servers may encounter unexpected power interruption as the batteries age and impact the availability.**

To take preventive action to mitigate this risk, which of the following should be considered most?

A. Mean Time Between Failure (MTBF)
B. Mean Time To Failure (MTTF)
C. Mean Time To Repair (MTTR)
D. Maximum Tolerable Downtime (MTD)

☞ Answer to QOTD: 20191226

275. **The incident response (IR) team in your company submitted an urgent human resource request for a security analyst. The job description of a security analyst requires at least five years of work experience and the CISSP certificate. Nawwar is an experienced network engineer with ten years of experience and the CISSP certificate. The head of the IR team proposed to hire Nawwar as soon as possible. As a security professional, which of the following suggestion will you make to the Human Resources department first?**

A. Make a contingent offer of employment
B. Ask for drug testing
C. Hire a professional organization to do a criminal background check
D. Conduct a reference check

☞ Answer to QOTD: 20191123

276. **The system administrator didn't exercise his due care neglecting the notification sent from the E-Commerce system that the RAID system is corrupting. Two RAID member disks failed in the end, that disrupted E-Commerce services. The company cannot tolerate such business losses over three days and shall recover the E-Commerce system in 24 hours.**

To recover the system, to which of the following should the system administrator refer?

A. Disaster Recovery Plan (DRP)
B. Business Continuity Plan (BCP)
C. Information System Contingency Plan (ISCP)
D. Computer Security Incident Response Plan (CSIRP)

☞ Answer to QOTD: 20191227

277. **The system administrator didn’t exercise his due care neglecting the notification sent from the E-Commerce system that the RAID system is corrupting. Two RAID member disks failed in the end, that disrupted E-Commerce services. Thanks to the established recovery strategy, the E-Commerce system automatically failed over to the alternative hot site in 10 minutes.**

Which of the following is the best to define the recovery strategy?

A. Disaster Recovery Plan (DRP)
B. Business Continuity Plan (BCP)
C. Information System Contingency Plan (ISCP)
D. Computer Security Incident Response Plan (CSIRP)

☞ Answer to QOTD: 20191228

278. **The system administrator didn't exercise his due care neglecting the notification sent from the E-Commerce system that the RAID system is corrupting. One RAID member disk failed in the end, which degraded the performance of E-Commerce services.**

The company cannot tolerate such business losses over three days and shall recover the E-Commerce system in 24 hours. Thanks to the inventory of spare hard drives, the failed hard drive can be replaced in 2 hours.

To recover the system, to which of the following should the system administrator refer?

A. Disaster Recovery Plan (DRP)
B. Computer Security Incident Response Plan (CSIRP)
C. Information System Contingency Plan (ISCP) subject to RTO greater than 12 hours
D. The hard drive replacement procedure

☞ Answer to QOTD: 20191229

279. **The system administrator didn't exercise his due care neglecting the notification sent from the E-Commerce system that the RAID system is corrupting. Two RAID member disks failed in the end, that disrupted the E-Commerce services. The company cannot tolerate such business losses over three days and shall recover the E-Commerce system in 24 hours. Thanks to the inventory of spare hard drives, the failed hard drive can be replaced in 2 hours.**

To recover the system, to which of the following should the system administrator refer?

A. Disaster Recovery Plan (DRP)
B. Computer Security Incident Response Plan (CSIRP)
C. Information System Contingency Plan (ISCP) with RTO greater than 12 hours
D. The hard drive replacement procedure

☞ Answer to QOTD: 20191230

280. **You learned from the news that the World Health Organization (WHO) is closely monitoring a novel deadly coronavirus under spreading. As a CISO, which of the following will you do first?**

A. Implement emergent update for latest antivirus signatures

B. Conduct the exercise of the Occupant Emergency Plan (OEP)
C. Enable the incident response plan and security incident response team
D. Review and test the business continuity plan (BCP)

☞ Answer to QOTD: 20200126

281. **As the World Health Organization (WHO) declared the novel coronavirus as a Public Health Emergency of International Concern (PHEIC) and officially renamed it to COVID 19, you are reviewing your contingent and continuity plans to prepare for the world-wide outbreak. Which of the following may least concern your organization when responding to the PHEIC in terms of business continuity?**

A. Disruption of supply chain
B. The convenience of remote access solutions
C. Effectiveness of redundant sites
D. Shortage of financial cash flow

☞ Answer to QOTD: 20200218

282. **You are developing a backup strategy to support the information system contingency plan (ISCP) that must meet the recovery time objective (RTO) and recovery point objective (RPO) determined in the business continuity plan (BCP). The full backup is scheduled at midnight on Sundays. It takes 7 hours to restore the full backup, differential or incremental backup would be restored afterward. Given the MTD (Maximum Tolerable Downtime) is 24 hours, RTO is 7 hours, and RPO is 1 hour, which of the following is the best decision?**

A. Perform a full backup on Sunday and incremental backups on every one hour.

B. Perform a full backup on Sunday and differential backups on every one hour.
C. Perform a full backup every day
D. Call a meeting to review the objectives

☞ Answer to QOTD: 20200225

283. **You are developing a backup strategy to support the information system contingency plan (ISCP) that must meet the recovery time objective (RTO) and recovery point objective (RPO) determined in the business continuity plan (BCP). The full backup is scheduled at midnight on Sundays. It takes 7 hours to restore the full backup, differential or incremental backup would be restored afterward. If the RTO is 24 hours and RPO is 1 day.**

Which of the following is the best decision in terms of backup efficiency?

A. Perform a full backup on Sunday and incremental backups on weekdays.
B. Perform a full copy backup on Sunday and incremental backups on weekdays.
C. Perform an incremental backup every one hour
D. Call a meeting to review the objectives

☞ Answer to QOTD: 20200301

284. **As a security professional, you are attending the risk management meeting. A member points out that a maintenance service provider for the ERP system is suffering financial problems that might hinder the service level. Which of the following should be conducted first?**

A. Escalate this problem to the management and suggest sourcing a backup provider

B. Activate the information system contingency plan (ISCP)
C. Train in-house team members to support the system as a backup solution
D. Identify affected business processes and related resources

☞ Answer to QOTD: 20200130

INCIDENT RESPONSE

285. **You are reviewing logs on a web server and find the following entry:**

[24/Feb/2020:00:05:36 +0800] "GET /load?image=../../../etc/shadow%00 HTTP/1.0" 200

Which of the following is the most possible vulnerability on the webserver?

A. The diagonal of the attack surface higher than risk appetite
B. Misconfiguration without due care
C. Continuous monitoring not automated by the "crond" daemon
D. Path traversal by adversaries

☞ Answer to QOTD: 20200224

286. **A network administrator responsible for monitoring network anomalies found, by analyzing network traffic, a sales representative sent an unencrypted email to competitors. It may involve price domination and violate antitrust. Which of the following is the best for the network administrator to convey this finding to appropriate management?**

A. Corporate bylaws
B. Acceptable use policy (AUP)
C. Crisis communication plan
D. Reporting procedure

☞ Answer to QOTD: 20200709

287. **You are the CISO of a multinational trading company. Your company implements a large scale web site selling products to global consumers. A network**

intrusion detection system (IDS) is implemented to detect abnormal traffic and potential attacks. Your incident response (IR) team receives a report from users that the web site is not available and shows HTTP error 404. An IR team member suspects that it's a distributed denial of service (DDOS) attack, but the IDS didn't trigger any alert. What action should the IR team take FIRST?

A. Document the incident in the incident management system.
B. Inform and ask the contracted internet service provider to mitigate the DDOS traffic
C. Analyze the incident report from the end-user and notify the senior management
D. Ask for more details from the end-user to realize the real situation

☞ Answer to QOTD: 20190422

288. **You are the CISO of your company. You have implemented an incident response program to handle security incidents. The on-premise ERP system gets in trouble and becomes unresponsive. The availability of the ERP system has been harmed. To which of the following should the ERP users report this incident?**

A. Service Desk
B. Network Administrator
C. Chief Information Officer (CIO)
D. Computer Security Incident Response Team (CSIRT)

☞ Answer to QOTD: 20190814

289. **You are the CISO of your company. You have implemented an incident response program to handle security incidents.**

Your online e-commerce web site is suffering a distributed denial-of-service (DDoS) attack. The incident response team received a report from users that the e-commerce web site is offline and unreachable.

What should the incident response team do first?

A. Collect and preserve evidence
B. Report to the senior management
C. Document and prioritize the incident
D. Contain, Eradicate, and Recover

☞ Answer to QOTD: 20190815

290. **Your company is selling toys online; the business is supported by an e-commerce web application developed in-house. Alice is the software developer of the development team who is in charge of the online EC system.**

The latest software release has just been approved by the management and deployed by Bob, who is a member of the operations team and responsible for the system operations.

Cherry bumped into an error message, HTTP 500 Internal Server Error, out of the blue, and turned to Alice asking for support. Alice told Cherry she should go for Bob, so much so that Cherry is complaining that Alice is irresponsible and pushing things away.

As a security professional, which of the following is the best way to deal with this situation?

A. Do nothing. Let Cherry go to Bob for help.
B. Give Alice a soft reminder to be responsible as she is the developer in charge.
C. Escalate the incident to Alice's supervisor.

D. Notify the human resource department to keep a record of this misconduct.

☞ Answer to QOTD: 20190913

291. **The incident response (IR) team in your company submitted an urgent human resource request for a security analyst. The job description of a security analyst requires at least five years of work experience and the CISSP certificate. Nawwar is an experienced network engineer with ten years of experience and the Cisco Certified Network Professional certificate. The head of the IR team proposed to hire Nawwar as soon as possible. As a security professional, which of the following suggestion will you make to the Human Resources department?**

A. Reject. Nawwar is incompetent.
B. Reject. The demand for security analysts is not urgent.
C. Accept. The IR team can conduct cross-training.
D. Accept. It's a regular practice of job rotation.

☞ Answer to QOTD: 20191122

292. **Your company, based in Taiwan and accredited with ISO 27001, sells toys online and ships globally. After conducting penetration testing, as part of the risk assessment, your company finished implementing honeypots solutions as security controls to deter and detect intruders. As a security professional, which of the following upcoming activities will you suggest your company do first?**

A. Conduct risk assessment
B. Research applicable laws and regulations
C. Implement consent banners and harden the honeypots to avoid entrapment

D. Create policies that define and clarify the goal of the honeypot system

☞ Answer to QOTD: 20200324

293. **Incident response is one of the major organizational capabilities. As an information security manager, you are developing the incident management plan for incident response.**

Which of the following is the least concern?

A. Computer forensics
B. Call tree
C. Spokesperson
D. Relocation

☞ Answer to QOTD: 20200514

294. **You are the CISO at Wonderland county government. The incident response team reports to you that unknown ransomware has successfully attacked the county's file servers and encrypted production data.**

As a CISO, which of the following do you think the IR team should conduct next?

A. Identify the root cause and remediate the problem
B. Prioritize the incident
C. Isolate infected machines
D. Validate if the incident is true

☞ Answer to QOTD: 20200624

DISASTER RECOVERY

295. **In an executive meeting, the vice president (VP) of manufacturing, the data owner of the material requirement planning (MRP), and the VP of sales, the data owner of the online shopping website, are justifying the criticality of the underlying information systems that process their data and support their business processes.**

Both of them believe their business processes are more critical and should be recovered first in case of a disaster.

As a CISO, how should you do?

A. Facilitate the process for the determination of the maximum tolerable downtime, and invite the VP of information technology to commit to the recovery time objective and recovery point objective.
B. Take importance and urgency into consideration, and implement a hot site for the business processes with higher priority during a code site for the ones with lower priority.
C. Prepare a disaster recovery plan (DRP) based on the recovery time objective and recovery point objective.
D. Prepare a business continuity plan (BCP) and a business case with alternatives to implement a hot site to support both MRP and the online shopping website.

☞ Answer to QOTD: 20190430

296. **After risk assessment, your company assigned you to prepare a disaster recovery plan to handle the identified disasters. A hot site, warm site, and cold site are common alternatives to the primary site. You are considering the backup site alternatives when preparing the disaster recovery plan.**

Which of the following will be your most concern?

A. Risk Appetite
B. Management Buy-in
C. Maximum Tolerable Downtime
D. Recovery Time Objective

☞ Answer to QOTD: 20190820

297. **The legacy Storage Area Network (SAN) storage went out of order and disrupted the ERP system of your company. As the lack of inventory for this legacy storage model, it takes two days to get a new one and recover the system. The contingency plan for this system is activated.**

Which of the following interim measures is least likely adopted?

A. Implementation of redundant information system functions
B. Recovery of information system functions using alternate equipment
C. Performance of information system functions using manual methods
D. Relocation of information systems and operations to an alternate site

☞ Answer to QOTD: 20191231

CHANGE MANAGEMENT

298. **Your company establishes a security baseline that requires all laptop computers shall be provisioned with biometric authentication. However, a small portion of outdated laptops that support token-based authentication only cannot meet the requirement.**

If the security baseline must be tailored to cover the laptops, which of the following actions should be taken first?

A. Submit a change request
B. Implement token-based authentication as the compensating control
C. Justify the request for the exception to the current security baseline
D. Communicate the performance to the management

☞ Answer to QOTD: 20200508

299. **Your company decides to sell toys online worldwide, which will be supported by a three-tiered web-based E-Commerce system developed in-house.**

The web servers for the production environment have been implemented but not baselined and approved by the management.

After the stress testing, the system engineer proposes that the memory size of the database server should be expanded to 64GB to meet the performance target.

If the memory modules needed are available, which of the following should the system engineer do first?

A. Install the memory modules and conduct another run of stress testing
B. Submit a request for configuration change

C. Justify the change to the change control board (CCB)
D. Document security implications in the change request

☞ Answer to QOTD: 20200525

DOMAIN 8: SOFTWARE DEVELOPMENT SECURITY

INITIATION AND PLANNING

300. **Your company decides to start the business of selling toys online and shipping globally. A software development team in-house is in charge of developing a web-based E-Commerce system that supports the new business. You are assigned as the project manager of the software development project. Which of the following artifact is the source of authority for your assignment?**

A. Master project management plan
B. Project charter
C. Software development policy
D. Business case

☞ Answer to QOTD: 20191214

301. **Your company decides to start the business of selling toys online and shipping globally. The E-Commerce system that supports the new business will be developed in-house. The COO, who doesn't like surprises, sponsors this initiative, and the reliability of the production system is the priority. He asked for periodic review and demonstration of development progress or prototypes and thought the daily standup meeting is favorable. The project team is evaluating the development approach. Which of the following is the best?**

A. Waterfall Model
B. Agile
C. Spiral Model
D. SCRUM

☞ Answer to QOTD: 20191030

302. **Your company decides to start the business of selling toys online and shipping globally. An in-house development team is tasked to develop the E-commerce system to support the new business. As a security professional and a member of the project team, you want to ensure the use of secure information system development processes.**

Which of the following provides practices or guidelines that best meet your requirements?

A. Agile
B. ISO 15288
C. NIST SP 800-160 Volume 1
D. CMMI

☞ Answer to QOTD: 20191223

303. **As a CISSP working for a direct bank based in Taiwan that relies entirely on internet banking, you are collaborating with the software development team of the customer relationship management (CRM) system to address security concerns.**

Which of the following approaches or standards will you least likely to employ?

A. Security function
B. XP (eXtreme Programming)
C. ISO 15288
D. The Sherwood Applied Business Security Architecture (SABSA)

☞ Answer to QOTD: 20200123

304. **The Secure Software Development Lifecycle (SSDLC) is curial to information security. The Agile mindset, which comprises a set of values, principles, and practices, is prevalent in software development.**

Scrum is one of the most well-known Agile practices nowadays.

Which of the following statements about Scrum is not true?

A. Scrum is a methodology that incorporates eXtreme Programming (XP) and Kanban.
B. The Product Owner is responsible for maximizing the value of the product.
C. The Development Team is self-organizing, so no one should tell them how to create values.
D. The Scrum Master is a servant-leader and helps everyone understand Scrum.

☞ Answer to QOTD: 20200423

305. **An Integrated Product Team (IPT) is a multidisciplinary group of people who are collectively responsible for delivering a defined product or process. Which of the following statements about the IPT is true?**

A. The structure of IPTs solely relies on the Work Breakdown Structure (WBS).
B. The composition of IPTs is favorable to the formation of Agile teams.
C. IPTs are system engineering teams, not responsible for acquisitions.
D. IPTs emphasize team diversity and don't fit classified military-based projects.

☞ Answer to QOTD: 20200422

NEEDS AND REQUIREMENTS

306. **Your company decides to sell toys online and ships globally. The target customers are house-hold consumers. An in-house team is responsible for developing the online shopping website.**

To maximize security assurance and market share, which of the following is the least concern?

A. The selection of computer languages
B. The adoption of Unified Modeling Language (UML)
C. The choice of the Software Development Life Cycle (SDLC)
D. The design of software architecture

☞ Answer to QOTD: 20200310

307. **Your company decides to start the business of selling toys online and shipping globally. The E-Commerce system that supports the new business will be developed in-house by an integrated product team (IPT). In a meeting, the IPT is discussing the solution using UML diagrams from a variety of views, such as user, logical, process, implementation, and deployment views.**

Which of the following is the IPT doing?

A. Feasibility analysis
B. Requirement analysis
C. Developing User Requirement Specification (URS)
D. Design review

☞ Answer to QOTD: 20191004

308. **Your company decides to start the business of selling toys online and shipping globally. The E-Commerce**

system that supports the new business will be developed in-house. The development team is designing the software architecture that shall be secure, scalable, responsive, and easy to maintain to support global operations.

Which of the following is the least appropriate?

A. Divide concerns into four layers but deploy the solution in three tiers
B. Follow open design and use an open cipher to encrypt confidential data
C. Require strong passwords at least 15 characters to ensure security
D. Validate privileges with the price of the performance every time access occurs

☞ Answer to QOTD: 20191009

309. **You are the project manager of a software development team following a generic software development life cycle. Meeting the requirements of stakeholders is crucial to the success of the project.**

Which of the following should be completed right before your team gets started to design the solution?

A. Requirement verification
B. Requirement certification
C. Requirement validation
D. Requirement analysis

☞ Answer to QOTD: 20200424

ARCHITECTURE AND DESIGN

310. **Your company develops security products. You are the head of the firewall product line and decide to develop a new firewall model based on formal designs. Which of the following best supports the design for the product?**

A. Use a prescribed system development life cycle (SDLC) compliant with standards
B. Follow the design principle of encapsulation and modulization and best practices
C. Employ a state machine and ensure secure transit between states
D. Gain certification from third-party evaluation for assurance

☞ Answer to QOTD: 20200621

311. **Your company decides to start the business of selling toys online and shipping globally. The E-Commerce system that supports the new business will be developed in-house by an integrated product team (IPT). In a meeting, the COO is concerned with performance issues resulting in loss of customer orders because of transaction timeout or customer impatience. Which of the following is the most appropriate to address this concern?**

A. Use client scripts to simulate customer's behavior
B. Conduct Fagan analysis to ensure source code is optimal
C. Install a debugger to monitor the performance of the production system
D. Implement a content distribution network to offload web server performance

☞ Answer to QOTD: 20191007

312. **Your company decides to start the business of selling toys online and shipping globally. The E-Commerce system that supports the new business will be developed in-house.**

In a threat modeling meeting, the development team identified a design flaw that might result in SQL injection attacks. The solution is a typical 3-tier architecture, the webserver farms for front-end presentation, elastic application server clusters for business logic, and database cluster for data persistence. The risk shall be addressed at the first priority after evaluation.

As a security professional, which of the following is the best suggestion?

A. For front-end UX programmers to validate user inputs
B. For back-end web programmers to validate user inputs
C. For the solution architect to design a secure architecture
D. For back-end web programmers to authenticate and authorize every HTTP request

☞ Answer to QOTD: 20191022

313. **Your company decides to start the business of selling toys online and shipping globally. A team in-house is in charge of developing an E-Commerce system that supports the new business. The procurement manager requests that the original purchase cost of products shall not be disclosed to other departments except procurement staff. Which of the following is the least feasible?**

A. Implement views for different roles
B. Display constrained user interface for unauthorized users
C. Enable the table that contains records with the same

primary keys to implement polyinstantiation
D. Develop a specific program dedicated to the procurement staff

☞ Answer to QOTD: 20191118

314. **Your company sells toys online worldwide. A web-based E-Commerce system developed by an in-house Integrated Product Team (IPT) supports the business. The development team is considering a solution to protect customer orders in motion. Which of the following is the best solution in terms of security, performance, and cost/benefit ratio?**

A. For developers to implement encryption in the business logic layer for full mediation
B. For the architect to incorporate a software encryption module as a cross-cutting aspect
C. For database administrators to implement a secure enclave on the database server
D. For web server administrators to enable secure transmission

☞ Answer to QOTD: 20200627

315. **You are writing code to develop a server that receives logs from a massive number of IoT devices for training the machine learning model. If every client establishes a connection to the server, it will hinder the scalability of the system. However, the amount of data is critical to the reliability of the model.**

Which of the following is the best solution?

A. Enable HTTP Keep-Alive to prevent from data loss
B. Ensure the accountability to trace back to the subject
C. Have the server listen to UDP port
D. Implement a SIEM server to train the model

☞ Answer to QOTD: 20200606

316. **Which of the following operations of a RESTful API that conforms to the REpresentational State Transfer (REST) architectural style most likely suffers from misuse cases by end-users?**

A. PUT
B. POST
C. GET
D. DELETE

☞ Answer to QOTD: 20200415

ACQUISITION AND DEVELOPMENT

318. **Your organization decides to implement an on-premise CRM system that will be supported and maintained by a service provider under a two-year fixed-price service contract. To cope with the business dynamics and stay flexible, which of the following is the best contract arrangement to engage with the service provider?**

A. Specify service level requirements (SLR) in the service contract
B. Separate the service level agreement (SLA) from the service contract
C. Preserve the right to audit to enforce supply chain security
D. Require only competent and certified engineers to fulfill this contract

☞ Answer to QOTD: 20200221

319. **Your company decides to start the business of selling toys online and shipping globally. The E-Commerce system that supports the new business will be developed in-house, while portions of the solution will be outsourced to an external software vendor. The project team is evaluating software outsourcing candidates. As a security professional, which of the following is the least concern?**

A. The financial history
B. Foreign ownership, control, and influence
C. Key escrow agreement
D. Right to conduct code reviews

☞ Answer to QOTD: 20191020

320. **Your company decides to sell toys online and ships globally. An in-house team is responsible for developing the online shopping website, while an external software vendor will subcontract some modules. The management is concerned about the vendor's software development capability.**

If the modules are outsourced as a project, which of the following vendor selection criteria best addresses the management's concern?

A. Projects are well-organized, executed, and repeatedly delivering results
B. Projects are managed proactively based on customizable organization-wide approaches
C. Projects are led by experienced, well-trained, and certified project managers.
D. Projects are awarded to a vendor with strong customer references and word of mouth

☞ Answer to QOTD: 20200323

321. **Your company decides to engineer an information system in-house to support the new business of selling toys online.**

The development team is in the process of selecting the compiled programming language to develop the back-end system, which deals with the business logic and data access and will be evaluated in terms of performance, availability, scalability, security, maintenance, and extensibility, while security is the most concern.

Which of the following is the most appropriate?

A. C++
B. Python

C. Java
D. JavaScript with Node.js

☞ Answer to QOTD: 20190921

322. **You are the head of the research and development department in charge of web conferencing products. The development team develops the product using an object-oriented language.**

Which of the following object-oriented principles or features relies on interfaces to decouple dependencies and exchange messages and achieve loose coupling?

A. Inheritance
B. Middleware
C. Polymorphism
D. Application Programming Interface (API)

☞ Answer to QOTD: 20200626

323. **Your company decides to start the business of selling toys online and shipping globally. The E-Commerce system that supports the new business will be developed in-house.**

The development team is developing the front-end user experience (UX) using JavaScript and evaluating solutions to protect the client scripts from being comprehended or investigated.

Which of the following is the best to do so?

A. Native code compiler
B. Obfuscator
C. Symmetric cipher
D. Code signing

☞ Answer to QOTD: 20191027

324. **Your company decides to sell toys online and ships globally. An in-house team is responsible for developing the online shopping website.**

The management requires that the front-line warehouse staff shall not have access to the product price of customer's purchase orders.

As a developer, which of the following is the most efficient technical control to address this requirement?

A. Polyinstantiation
B. Restricted database views
C. Constrained interface
D. Access control policy

☞ Answer to QOTD: 20200316

TESTING AND DEPLOYMENT

326. **Your company decides to sell toys online and ships globally. An in-house team is responsible for developing the online shopping website.**

To improve software security and quality, which of the following is the best role responsible for writing unit tests?

A. Software developer
B. Software tester
C. End-user
D. Continuous integration (CI) server

☞ Answer to QOTD: 20200315

327. **An aircraft manufacturer is suffering a harsh situation that two aircraft crashed, causing hundreds of deaths, because of the defect of the flight control software system outsourced to the offshore software vendor.**

As a security professional, which of the following is the best to improve the software quality to avoid this tragedy?

A. Code review
B. Regression testing
C. Formal inspection
D. Agile testing

☞ Answer to QOTD: 20200106

328. **Your company decides to sell toys online and ships globally. An in-house software development team is responsible for developing the online shopping website, and a software testing strategy is under consideration.**

Which of the following statement about software testing is true?

A. Unit testing is an automated black-box testing technique
B. User interface testing is black-box testing that requires manual data input
C. Fuzzing testing is a passive automated testing technique
D. Synthetic testing is a dynamic automated testing technique

☞ Answer to QOTD: 20200327

329. **Your company is an independent software vendor (ISV), providing software packages with the click-through license agreement.**

Which of the following testing is most likely conducted before providing global availability (GA)?

A. Beta testing
B. User acceptance testing (UAT)
C. Regression testing
D. Installation testing

☞ Answer to QOTD: 20200426

330. **Your company develops security products. You are the head of the firewall product line and decide to develop a new firewall model. Formal methods will be used for specification, verification, and other aspects of product development.**

Which of the following is not a formal method?

A. Fagan inspection
B. Delphi method
C. Lattice-based access control
D. Finite-state machine

☞ Answer to QOTD: 20200622

331. **Your company decides to start the business of selling toys online and shipping globally. A team in-house is in charge of developing an E-Commerce system that supports the new business. The software development team is implementing the web service in the RESTful style. The software testing team is testing a user story, "As a customer, I want to place an order so that I can buy a toy." It passed in the testing/lab environment but failed in the staging environment.**

Which of the following is the most likely reason?

A. The firewall allows the GET method only
B. The intrusion detection system (IDS) misjudged the transaction as a CSRF attack
C. The intrusion prevention system (IPS) allows the POST method only
D. The back-end web server validates every input value

☞ Answer to QOTD: 20191107

332. **Your company decides to start the business of selling toys online and shipping globally. A team in-house is in charge of developing an E-Commerce system that supports the new business. The software testing team reported a bug that users cannot change passwords after signing in. The development team fixed the bug and asked for testing. However, the software testing team reported another bug that users cannot sign in to the system.**

Which of the following best describes the testing that should have been conducted?

A. Code review
B. Regression testing

C. Automated UI testing
D. Integration testing

☞ Answer to QOTD: 20191106

333. **You are the development team leader and recently found your nightly build failed from time to time. Eve was a disgruntled developer in your team and quit last month. She is responsible for part of the solution and is not authorized to integrate the solution. She installed a program running under the local system privilege to delete, on Monday midnights, some source code in the local code repository pushed to the central code repository to be integrated. What is the program installed by Eve called?**

A. Encapsulation
B. Maintenance hook
C. Multipartite
D. Logic bomb

☞ Answer to QOTD: 20190823

334. **Your company decides to start the business of selling toys online and shipping globally. A team in-house is in charge of developing an E-Commerce system that supports the new business. As code quality is a priority, the development team decides to implement the unit testing.**

Which of the following is the best strategy in practice?

A. Task the software testing team to write unit testing code for separation of duty
B. Ask developers to write unit testing code before writing production code
C. Request developers to write unit testing code after writing production code

D. Demand the system analysts specify the unit testing specification before writing production code

☞ Answer to QOTD: 20191105

335. **You are managing a software development project and considering implementing DevOps.**

After doing some research, you realized that ISO/IEC TS 23167:2020 defines DevOps as the "methodology which combines together software development and IT operations in order to shorten the development and operations lifecycle."

Which of the following statements about DevOps is not true?

A. DevOps relies heavily on tools for automation and streamlining the processes.
B. Agile addresses communication gaps between customers and developers, while DevOps addresses gaps between developers and IT operations.
C. DevOps relieves the burden of security professionals by central management.
D. In addition to developers and system administrators, DevOps also engages QA staff.

☞ Answer to QOTD: 20200425

OPERATIONS AND MAINTENANCE

336. **Your company sells toys online worldwide, which is supported by a three-tiered web-based E-Commerce system. To avoid inconsistent system configurations, which of the following is the most important?**

A. Detail procedures
B. Up-to-date standards
C. Sound governance
D. Periodic training

☞ Answer to QOTD: 20200524

337. **Your company sells toys online worldwide. A web-based E-Commerce system developed in-house supports the business.**

The EC system comprises a web server farm to present the web user interface and application programming interface. A cluster of application servers handles user transactions. A primary RDBMS server with two secondary servers holding DB replica persists user transactions and enables cache operations.

Which of the following best describes the design of the deployment architecture?

A. Multi-layered model
B. Subject-Object model
C. Client/Server model
D. Multi-tiered model

☞ Answer to QOTD: 20200610

338. **Your company decides to start the business of selling toys online and shipping globally. The E-Commerce system that supports the new business will be developed in-house.**

The development team is planning for a DevOps solution. It conducts a nightly build for integration testing. If it completes successfully, other automated tests continue. If everything goes well, the software solution will be deployed to the production system automatically.

As the COO with reliability and availability at priority, which of the following best addresses your concern?

A. Deploy after conducting more testing to ensure software quality
B. Ask for manual deployment by the operation team to enforce separation of duty
C. Require the deployment be conducted after approval
D. Upgrade to cutting edge DevOps product to avoid vulnerabilities

☞ Answer to QOTD: 20191102

DATA PERSISTENCE AND DATABASES

339. **Your company decides to start the business of selling toys online and shipping globally. The E-Commerce system that supports the new business will be developed in-house.**

The development decides to use the relational database as the data persistence solution for transactions. One team member is tasked to design the database.

Which of the following is least likely to happen?

A. Assign one and only one primary key in each table
B. Keep the attributes related to the primary key and move unrelated ones to other tables
C. Use multiple attributes as the primary key in a relation
D. Avoid foreign key references the primary key in the master table to enforce integrity

☞ Answer to QOTD: 20191016

340. **Your company decides to start the business of selling toys online and shipping globally. The E-Commerce system that supports the new business will be developed in-house. The development team is implementing the data persistence solution based on the relational database. The customer privacy data and credentials shall be protected from the access of the database administrator (DBA).**

Which of the following best addresses the requirement?

A. Limit the DBA's access by joining tables into views
B. Use electronic codebook (ECB) cipher to protect data at

rest
C. Implement role-based access control (RBAC)
D. Enable TLS/SSL transportation between clients and the server

☞ Answer to QOTD: 20191019

341. **Your company decides to start the business of selling toys online and shipping globally. The E-Commerce system that supports the new business will be developed in-house. The development team is designing the data model for the SQL database based on the entity-relationship diagram. It splits the comma-separated values (CSV) data stored in a field into multiple fields.**

Which of the following best describes the process?

A. Split horizon
B. Normalization in 1NF
C. Normalization in 2NF
D. Key clustering

☞ Answer to QOTD: 20191029

342. **Which of the following is the best construct that reduces data redundancy in the relational database?**

A. Foreign key constraints
B. Database normalization
C. Primary key constraints
D. Data types and domain restriction

☞ Answer to QOTD: 20200331

343. **Your company sells toys online worldwide, which is supported by a three-tiered web-based E-Commerce system.**

The data tier is an active-passive high-availability cluster of RDBMS servers. A special-priced toy is hot selling so much so that only one is available in stock.

Two customers online concurrently place an order, and both receive a success response. The stock quantity becomes an unreasonable value, a negative one.

Which of the following is least helpful to mitigate the risk?

A. Isolation
B. The ACID principle
C. The * (star) Integrity Property
D. Concurrency control

☞ Answer to QOTD: 20200521

344. **You are developing an order processing system supported by an RDBMS and wrote a piece of SQL code as a transaction to update the customer's lifetime value as follows:**

```
1> UPDATE Customers SET LifeTimeValue = LifeTimeValue + 99
WHERE CustomerId = 1

2> UPDATE Invoices SET TotalAmount = 99 WHERE InvoiceId = 1
```

However, your colleague wrote the same code in the reverse sequence. If only your transaction succeeds its updates, which of the following has been hindered?

A. Entity integrity
B. Semantic integrity
C. Referential integrity
D. Availability

☞ Answer to QOTD: 20200711

345. **You are developing an order processing system supported by an RDBMS and wrote a piece of SQL code as a transaction to update the customer's lifetime value as follows:**

1> UPDATE Customers SET LifeTimeValue = LifeTimeValue + 99 WHERE CustomerId = 1

2> UPDATE Invoices SET TotalAmount = 99 WHERE InvoiceId = 1

However, your colleague wrote the same code in the reverse sequence. If a customer may have many invoices, which of the following will occur most likely?

A. Inference
B. Aggregation
C. Race condition
D. Loss of referential integrity

☞ Answer to QOTD: 20200710

346. **Your company decides to start the business of selling toys online and shipping globally. The E-Commerce system that supports the new business will be developed in-house. The development team is evaluating the data persistence solution for transactions. The solution shall support a huge volume of transactions, and the single point of failure shall be addressed.**

Which of the following will best address the requirements?

A. Key-value stores that support multi-node parallel computing
B. Snowflake tables in data marts supported by an active-passive server cluster
C. Data warehouse as big data storage with an active-active cluster

D. Attributes and tuples in relations with one primary and one standby server

☞ Answer to QOTD: 20191013

347. **Your company sells toys online and ships globally. Most developers of the development team for the online E-Commerce system are experienced ones.**

To prevent developers from writing code that is subject to SQL injection attacks, which of the following is the least effective?

A. Common Weakness Enumeration (CWE)
B. Common Vulnerabilities and Exposures (CVE)
C. Training
D. OWASP Top 10

☞ Answer to QOTD: 20200307

THREAT MODELING

348. **Your company decides to start the business of selling toys online and shipping globally.**

A software development team in-house has gone through analysis, design, development, and testing. Shortly after the E-Commerce system goes into operations, it suffers SQL injection attacks and data breach.

As a security professional, which of the following is the best strategy to conduct threat modeling to mitigate risks?

A. In the initial design stage
B. In the testing stage
C. As late as in the operations stage
D. All of the above

☞ Answer to QOTD: 20191218

349. **There is no consistent definition of "threat," and people tend to use this term literally or intuitively. As a threat may refer to the threat source, threat event, or risk exposure, which of the following is least likely to be a threat?**

A. Script kiddie
B. The financial loss of millions of dollars
C. Unpatched servers
D. Initiating SQL injection using SQLMap

☞ Answer to QOTD: 20200216

350. **Your company is engineering an information system to support the new business of selling toys online.**

As a security professional, you are working with the development team to review the design for flaws in the threat modeling process.

Which of the following will you LEAST use in the process of identifying potential threats or design flaws?

A. Misuse case
B. STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege)
C. DREAD (Damage, Reproducibility, Exploitability, Affected Users, and Discoverability)
D. CWE (Common Weakness Enumeration)

☞ Answer to QOTD: 20190831

351. **Your company decides to start the business of selling toys online and shipping globally. A team in-house is in charge of developing an E-Commerce system that supports the new business. In a meeting, you suggest that the solution shall not support legacy browsers and SSL even though it would lose the market coverage of browsers. As a security professional, which of the following is your primary concern to do so?**

A. To prevent web pages from distortion due to insufficient support of HTML5 and CSS3
B. To mitigate the threat exploiting the vulnerability of the heartbeat extension
C. To avoid attackers using the protocol padding vulnerability to decrypt the ciphertext.
D. To stop attackers from using the nonce to break the encryption key

☞ Answer to QOTD: 20191109

352. **Your company decides to start the business of selling toys online and shipping globally. A team in-house is in charge of developing an E-Commerce system that supports the new business. The software development team is implementing the web service in the RESTful style. HTTPS or TLS protects communication between browsers and webserver. Which of the following is the security issue that least concerns the software development team?**

A. Heartbleed
B. SQL Injection
C. Cross-Site Scripting (XSS)
D. Cross-Site Request Forgery (CSRF)

☞ Answer to QOTD: 20191108

353. **Your company decides to start the business of selling toys online and shipping globally. A team in-house is in charge of developing an E-Commerce system that supports the new business.**

The testing team was conducting dynamic application security testing (DAST) and activated the Calculator app, one of the Windows accessories, on one of the web servers through an input field in an HTML form. This test demonstrated a successful attempt of intrusion.

Which of the following is least feasible to prevent the attack?

A. Apply limit of the input length.
B. Enable Data Execution Prevention (DEP)
C. Enable Address Space Layout Randomization (ASLR)
D. Conduct Time-of-check to time-of-use (TOC/TOU) check

☞ Answer to QOTD: 20191121

354. **Your company decides to start the business of selling toys online and shipping globally. A team in-house is in charge of developing an E-Commerce system that supports the new business.**

SSL/TLS protects communication between browsers and web server farms. The performance tester observed that the CPU utilization of web servers kept as high as 100%, and some connections will time out.

However, the webserver farms work fine under HTTP connections. Moreover, the web servers are I/O bound in nature; they mostly accept file requests and dispatch transactions to the application server clusters.

Which of the following is most feasible to address the time-out and improve availability?

A. Increase the bandwidth, e.g., from T1 to T3.
B. Add more RAM/memory to improve system performance
C. Implement hardware security modules to offload processing
D. Upgrade to faster CPUs on each web server to speed up the processing

☞ Answer to QOTD: 20191119

355. **The system administrator found a logic bomb installed on a back-end server. It was alleged that the disgruntled former system administrator got involved.**

As a security professional, which of the following will you suggest first to prevent it from reoccurring?

A. Ask 5-Whys to investigate in-depth for the solution
B. Reinstall the server using the CD media
C. Conduct thorough reference check and background

investigation
D. Apply lessons learned for continuous improvement

☞ Answer to QOTD: 20200121

356. **As a CISSP working for a direct bank based in Taiwan that relies entirely on internet banking, you are participating in a development meeting for threat modeling the customer relationship management (CRM) system, a web application. A member identifies an attack vector that malicious users might manipulate query parameters in the URL resulting in a server buffer overflow.**

Which of the following should be conducted first?

A. Replace the static array as the buffer with a dynamic one
B. Refer to OWASP Top 10 for suggested solutions
C. Evaluate how easy for a malicious user to make it
D. Authenticate every user input

☞ Answer to QOTD: 20200125

357. **Which of the following programming constructs most likely suffers from the stack overflow attack?**

A. Static variables
B. Local variables
C. Global variables
D. Dynamically allocated buffers

☞ Answer to QOTD: 20200412

358. **Your company sells toys online worldwide, which is supported by a web-based E-Commerce system.**

The EC system issues an access token, which is renewed on a rolling basis, for subsequent access

authorization after a user is validated.

The front-end experience in modern web browsers is implemented by mobile code, which is supported by a RESTful back-end API with rigid input validation.

You are planning for a new feature that simplifies the process of placing orders by adding a "Buy it again" button beside each historical order.

Which of the following is the most concern?

A. Cross-Site Scripting (XSS)
B. Injection
C. Replay
D. Cross-Site Request Forgery (CSRF)

☞ Answer to QOTD: 20200520

359. **Your company sells toys online worldwide. A web-based E-Commerce system developed in-house supports the business. The EC system is suffering from the DDoS attack.**

Which of the following is the most effective mitigation strategy?

A. Enable the elastic network capability to deal with the massive amount of traffic
B. Implement a dynamic DNS to avoid the attack
C. Rotate the IPs of the web server farm in round-robin
D. Redirect the traffic to the scrubbing center

☞ Answer to QOTD: 20200608

360. **Your company decides to subscribe to a portfolio of software services as SaaS from a well-known cloud service provider.**

The program policy limits the consumption of software to business use only. Employees are not allowed to use the software at home or for personal use. As a security professional, you are tasked to assess the risk and propose solutions to mitigate risk.

Which of the following least contributes to the risk assessment process ?

A. Context diagram
B. Location-based authentication
C. OSINT (Open-source intelligence)
D. SDLC (System Development Life Cycle)

☞ Answer to QOTD: 20200708

361. **Your company sells toys online worldwide, which is supported by a three-tiered E-Commerce web-based system. As a security professional, you are participating in a threat modeling meeting.**

Which of the following is the least concern?

A. Processing in the business logic tier
B. Rendering output to the data tier
C. Accepting input from the presentation tier
D. Data flow between tiers

☞ Answer to QOTD: 20200513

362. **Your company decides to start the business of selling toys online and shipping globally. The software development is conducting threat modeling and identifies a misuse case that an attacker can manipulate the backend database by sending XML messages through HTTP POST.**

Which of the following vulnerability should be fixed first?

A. SQL Injection
B. XML External Entities (XEE)
C. Broken Authentication
D. Cross-Site Request Forgery (CSRF)

☞ Answer to QOTD: 20191219

363. **Your company sells toys online worldwide, which is supported by a three-tiered web-based E-Commerce system.**

To prevent CSRF (Cross-site request forgery) attack, which of the following is the most effective control?

A. Conduct awareness training
B. Submit transactions that change states through HTTP POST only
C. Append the hash value of transaction parameters to the query string
D. Put an authentication token in a hidden input in HTML forms in an obscure way

☞ Answer to QOTD: 20200522

364. **Your company sells toys online worldwide. A web-based E-Commerce system developed in-house supports the business. The EC system comprises a web server farm to present the web user interface and application programming interface.**

Which of the following is the best role to address the attacks of Cross-Site Scripting (XSS) and Cross-site request forgery (XSRF)?

A. The front-end developer who validates UI inputs
B. The back-end developer who filters out invalid characters
C. The database administrator who implements the parameterized query

D. The solution architect who designs the system architecture

☞ Answer to QOTD: 20200612

365. **Your company decides to start the business of selling toys online and shipping globally. The E-Commerce system that supports the new business will be developed in-house by an integrated product team (IPT).**

In a meeting, the IPT is discussing the solution using UML diagrams from a variety of views, such as user, logical, process, implementation, and deployment views.

Which of the following is least likely used in the meeting?

A. Use Cases
B. DREAD (Damage, Reproducibility, Exploitability, Affected Users, and Discoverability)
C. CWE (Common Weakness Enumeration)
D. Code Review

☞ Answer to QOTD: 20191005

ANSWER KEYS

DOMAIN 1: SECURITY AND RISK MANAGEMENT

DOMAIN 2: ASSET SECURITY

No	QOTD	Answer Key
52	20200628	A. All employees.
53	20190923	D. Define the classification scheme.
54	20190924	C. Have Cynthia in charge of the proposal.
55	20190925	C. Use the vendor-provided utility with the dedicated commands to purge all the data.
56	20190927	C. Data Controller.
57	20200208	C. Information stewardship.
58	20200212	B. Data custodian.
59	20200214	A. Commercial-Off-The-Shelf (COTS) software.
60	20200613	D. The IT manager and data owners.
61	20200707	D. The vice president of Sales, for the responsibility and authority of classification and protection.
62	20200705	C. Take inventory.
63	20191117	D. Data marking.
64	20200107	C. Business value.
65	20200210	A. Label the USB dongle at the highest level of sensibility.
66	20191101	D. Cryptographic Erase.
67	20200209	B. Write zeros in all bytes of logical sectors.
68	20200211	C. Strength of cryptographic algorithms.
69	20200220	A. Hierarchical storage management (HSM).
70	20191001	A. Consult the information system owner.
71	20191221	C. Technical.

DOMAIN 3: SECURITY ARCHITECTURE AND ENGINEERING

DOMAIN 4: COMMUNICATION AND NETWORK SECURITY

DOMAIN 5: IDENTITY AND ACCESS MANAGEMENT (IAM)

DOMAIN 6: SECURITY ASSESSMENT AND TESTING

No	QOTD	Answer Key
242	20200420	D. Security assessment.
243	20200119	D. Security control assessment.
244	20200219	C. Testing.
245	20200528	B. Security assessment.
246	20200429	C. Open Source Security Testing Methodology Manual (OSSTMM).
247	20200104	C. Business case.
248	20200427	B. Conduct passive testing against the target.
249	20200428	C. Conduct OSINT (Open-source intelligence).
250	20200430	B. Prepare follow-up report for management review and decision.
251	20200511	D. Threat modeling.
252	20200529	C. The procedure that the penetration test team asks for permission to conduct penetration test.
253	20200607	C. A list of network hosts.
254	20200404	C. Conduct risk assessment.
255	20190919	C. Conduct penetration testing to validate the security controls.
256	20200109	D. Is risk assessment conducted before business impact analysis.
257	20200110	B. SOC 2 Type I.
258	20200114	A. Development progress of the business continuity plan.
259	20200115	D. Collaborate with the audit department.
260	20200116	A. Employing the Delphi method.
261	20200124	C. (ISC)2 Code of Ethics.
262	20200502	C. Type 1 SOC 2.
263	20200813	D. Self-assessment.
264	20200814	B. Baselines.

DOMAIN 7: SECURITY OPERATIONS

DOMAIN 8: SOFTWARE DEVELOPMENT SECURITY