1. True or False. A security architect's job is to make sure that security considerations are balanced against other design aspects such as usability, resilience and cost. — 1 point
   - (•) True
   - ( ) FALSE

2. Which of these is an aspect of an Enterprise Architecture? — 1 point
   - (•) Maps the main components of a problem space and solution at a very high level.
   - ( ) Gives the technology perspectives in detail
   - ( ) Describes how specific products or technologies are used
   - ( ) Shows the internal data and use of reusable or off-the-shelf components

3. Which of these is an aspect of a Solution Architecture? — 1 point
   - (•) Shows the internal data and use of reusable or off-the-shelf components
   - ( ) Does not describe the internals of the main components or how they will be implemented
   - ( ) Maps the main components of a problem space and solution at a very high level
   - ( ) Considers the needs of the entire organization

4. Which three (3) of these are features of Architecture Building Blocks (ABBs)? (Select 3) — 1 point
   - [ ] Specifies the technical components to implement a function
   - [x] Guides the development of a Solution Architecture
   - [x] Captures and defines requirements such as function, data, and application
   - [x] Product and vendor neutral

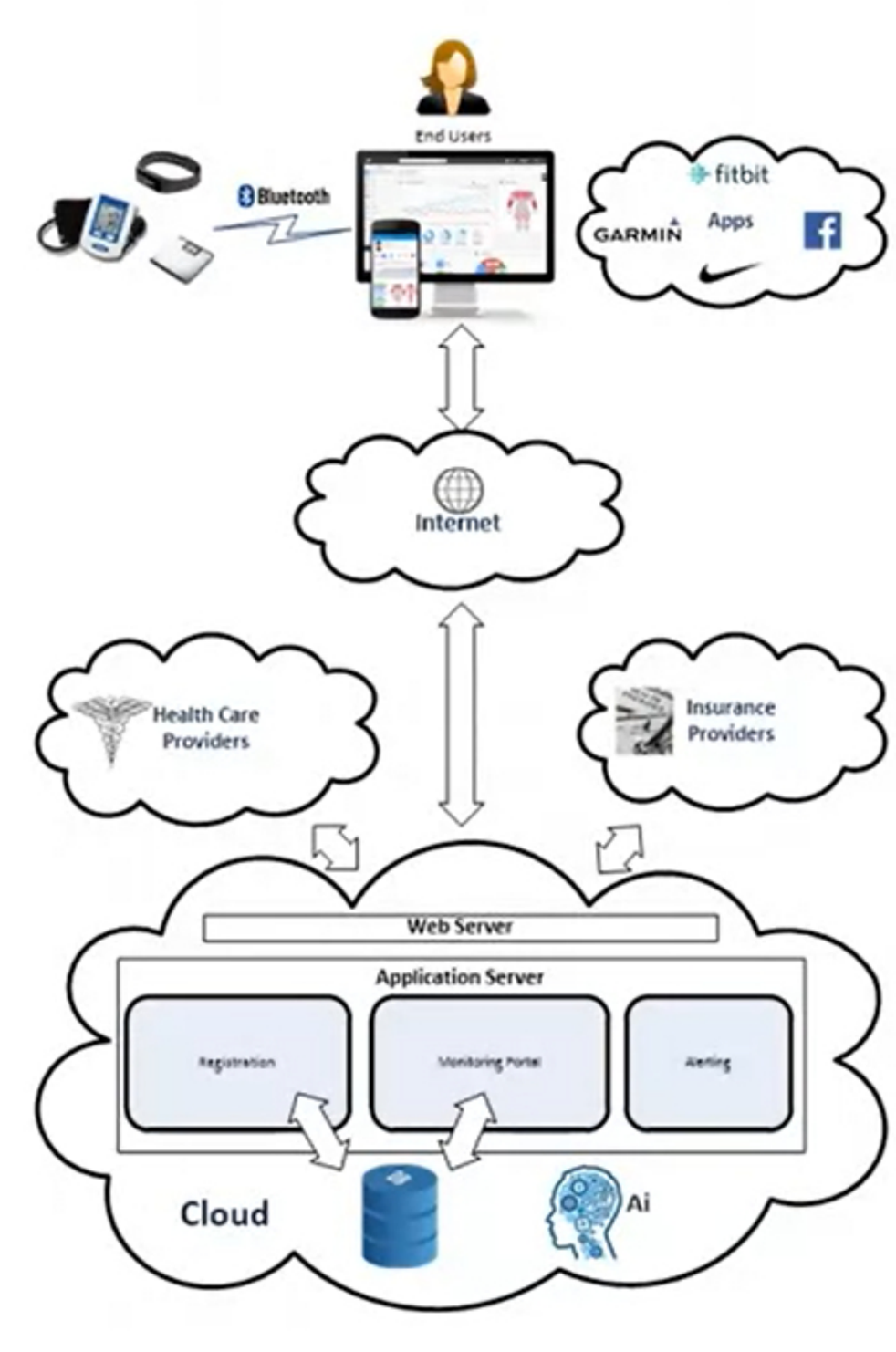
5. Which three (3) of these are Architecture Building Blocks (ABBs)? (Select 3) — 1 point
   - [ ] Key Security Manager
   - [x] Detect and Respond
   - [x] Identity and Access Management
   - [x] Infrastructure and Endpoint Security

6. Which three (3) of these are Solution Building Blocks (SBBs)? (Select 3) — 1 point
   - [x] Privilege Access Manager
   - [x] Hardware Token
   - [ ] Application Security
   - [x] Web Application Firewall (WAF)

7. The diagram below shows which level of architecture? — 1 point

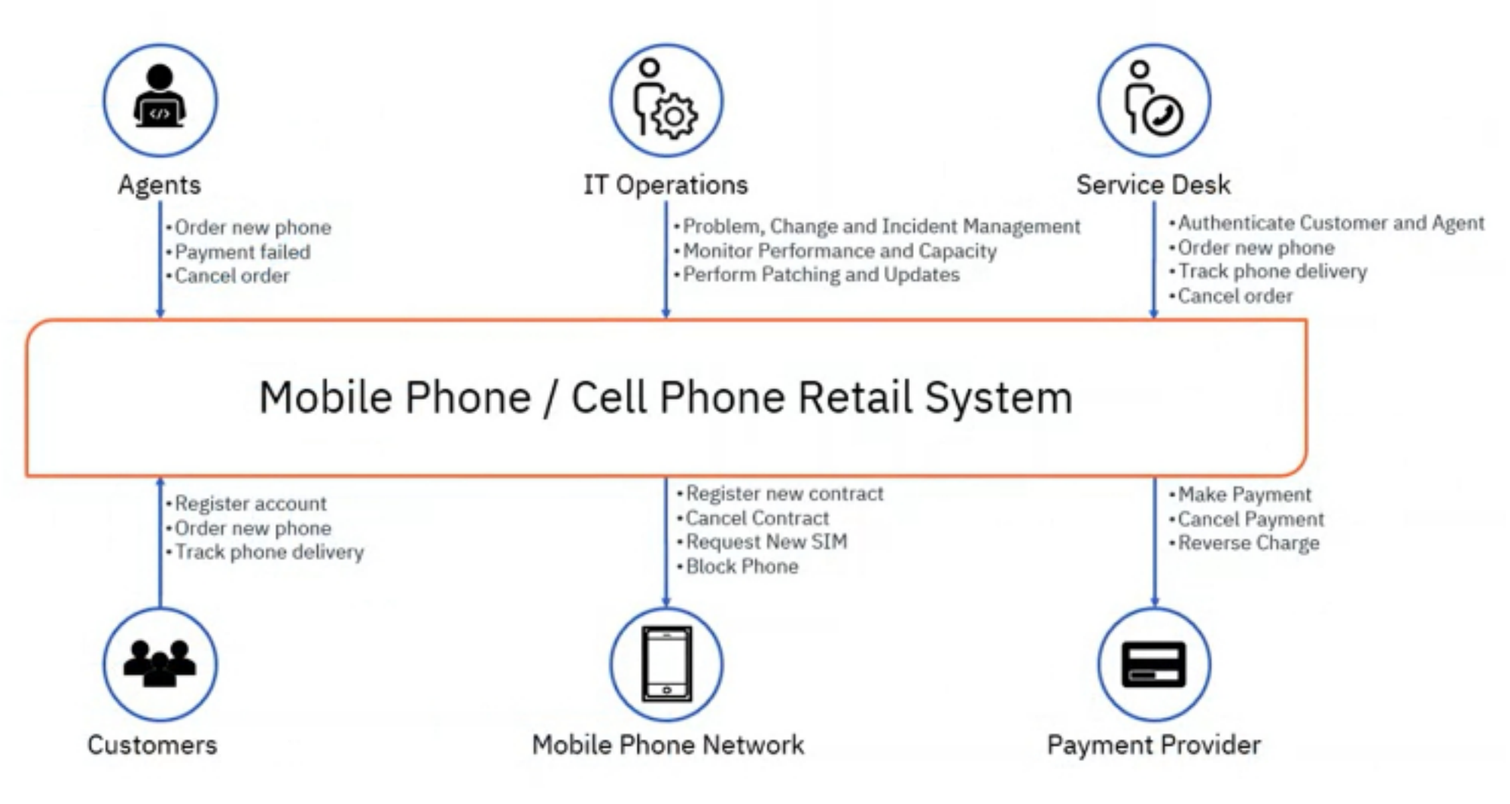
   - ( ) High Level Security Architecture
   - (•) Enterprise Security Architecture
   - ( ) Domain-specific Enterprise Security Architecture
   - ( ) Solution Architecture

8. Solution architectures often contain diagrams like the one below. What does this diagram show? — 1 point



   - (•) Solution architecture overview
   - ( ) Functional components and data flow
   - ( ) External context and boundry diagram
   - ( ) Enterprise architecture

9. Solution architectures often contain diagrams like the one below. What does this diagram show? — 1 point



   - ( ) Functional components and data flow
   - ( ) Enterprise architecture
   - ( ) Architecture overview
   - (•) External context and boundary diagram

10. What is lacking in a security architecture pattern that prevents it from being used as a finished design? — 1 point
    - ( ) Proper level of abstraction
    - (•) The context of the project at hand
    - ( ) Vendor selections
    - ( ) Proper formatting

11. What are the possible consequences if a bug in your application becomes known? — 1 point
    - ( ) It is embarrassing to your company
    - ( ) Financial losses via lawsuits and fines can be very significant
    - ( ) Government agencies can impose fines and other sanctions against your company
    - (•) All of the above

12. What was the ultimate consequence to Target Stores in the United States from their 2013 data breach in which over 100M records were stolen? — 1 point
    - (•) Costs and fines estimated at $1B.
    - ( ) Costs of $10M and reputational damage only.
    - ( ) Criminal negligence charges were filed 3 Target executives, 1 of whom received a prison sentence
    - ( ) Costs and fines that forced the company into bankruptcy

13. Select the two (2) top vulnerabilities found in common security products. (Select 2) — 1 point
    - [x] Cross-site request forgery
    - [ ] Use of hard-coded credentials
    - [x] Cross-site scripting
    - [ ] SQL Injection

14. True or False. If you can isolate your product from the Internet, it is safe from being hacked. — 1 point
    - ( ) True
    - (•) False

15. Which three (3) things can Cross-site scripting be used for? (Select 3) — 1 point
    - [ ] Break encryption
    - [x] Harvest credentials
    - [x] Take over sessions
    - [x] Steal cookies

16. True or False. Commonly a Reflect XSS attack is sent as part of an Email or a malicious link and affects only the the user who receives the Email or link. — 1 point
    - (•) True
    - ( ) False

17. Cross-site scripting attacks can be minimized by using HTML and URL Encoding. How would a browser display this string?: — 1 point

    Password

    - ( ) Password
    - (•) Password
    - ( ) <<Password>>
    - ( ) **Password**

18. Which three (3) statements about whitelisting user input are true? (Select 3) — 1 point
    - [ ] Single quotes should never be allowed as user input
    - [x] Whenever possible, input should be whitelisted to alphanumeric values to prevent XSS
    - [x] Special characters should only be allowed on an exception basis
    - [x] Whitelisting reduces the attack surface to a known quantity

19. Which two (2) statements are considered good practice for avoiding XSS attacks (Select 2) — 1 point
    - [ ] Use blacklists and client-side validation
    - [x] Encode all data output as part of HTML and JavaScript
    - [x] Use strict whitelists on accepting input
    - [ ] Develop you own validation or encoding functionality that is customized for your application

20. How would you classify a hactivist group who thinks that your company's stance on climate change threatens the survival of the planet? — 1 point
    - ( ) A vector
    - ( ) A vulnerability
    - ( ) A risk
    - (•) A threat

21. Which software development lifecycle is characterized by short bursts of analysis, design, coding and testing during a series of 1 to 4 week sprints? — 1 point
    - ( ) Spiral
    - (•) Agile and Scrum
    - ( ) Waterfall
    - ( ) Iterative

22. Which software development lifecycle is characterized by a series of cycles and an emphasis on security? — 1 point
    - (•) Spiral
    - ( ) Agile and Scrum
    - ( ) Waterfall
    - ( ) Iterative

23. Which form of penetration testing allows the testers no knowledge of the systems they are trying to penetrate in advance of their attack to simulate an external attack by hackers with no knowledge of an organizations systems? — 1 point
    - (•) Black Box Testing
    - ( ) Red Box Testing
    - ( ) White Box testing
    - ( ) Gray Box Testing

24. Which application testing method requires a URL to the application, is quick and cheap but also produces the most false-positive results? — 1 point
    - (•) DAST: Dynamic Security Application Testing
    - ( ) PAST: Passive Application Security Testing
    - ( ) SAST: Static Application Security Testing
    - ( ) IAST Interactive Application Security Testing

25. Which type of application attack would include buffer overflow, cross-site scripting, and SQL injection? — 1 point
    - ( ) Authorization
    - ( ) Configuration management
    - (•) Input validation
    - ( ) Authentication

26. Which type of application attack would include unauthorized access to configuration stores, unauthorized access to administration interfaces and over-privileged process and service accounts? — 1 point
    - ( ) Auditing and logging
    - (•) Configuration management
    - ( ) Exception management
    - ( ) Authentication

27. Which one of the OWASP Top 10 Application Security Risks would occur when authentication and session management functions are implemented incorrectly allowing attackers to compromise passwords, keys or session tokens. — 1 point
    - ( ) Sensitive data exposure
    - ( ) XML external entities (XXE)
    - (•) Broken authentication
    - ( ) Broken access control

28. Which one of the OWASP Top 10 Application Security Risks would occur when restrictions on what a user is allowed to do is not properly enforced? — 1 point
    - ( ) Security misconfiguration
    - ( ) Cross-site scripting
    - ( ) Insecure deserialization
    - (•) Broken access control

29. Which of these threat modeling methodologies is integrated seamlessly into an Agile development methodology? — 1 point
    - ( ) TRIKE
    - ( ) STRIDE
    - (•) VAST
    - ( ) P.A.S.T.A.

30. Security standards do not have the force of law but security regulations do. Which one of these is a security regulation? — 1 point
    - ( ) ISO 27034/24772
    - (•) HIPAA
    - ( ) NIST 800-53
    - ( ) PCI-DSS

31. Which phase of DevSecOps would contain the activities Secure application code, Secure infrastructure configuration, and OSS/COTS validation? — 1 point
    - ( ) Plan
    - (•) Code & build
    - ( ) Operate & monitor
    - ( ) Test
    - ( ) Release, deploy & decommission

32. Which phase of DevSecOps would contain the activities Detect & Visualize, Respond, and Recover? — 1 point
    - (•) Operate & monitor
    - ( ) Code & build
    - ( ) Release, deploy & decommission
    - ( ) Plan
    - ( ) Test

33. The Deploy step in the DevSecOps Release, Deploy & Decommission phase contains which of these activities? — 1 point
    - ( ) Versioning of infrastructure
    - ( ) IAM controles to regulate authorization
    - ( ) Data backup cleansing
    - (•) Creation of Immutable images

34. The Respond step in the DevSecOps Operate & Monitor phase contains which of these activities? — 1 point
    - ( ) Root Cause Analysis
    - ( ) Chaos engineering
    - ( ) Inventory
    - (•) Virtual Patching