Standards that
create the outstanding

BCS Practitioner Certificate in Information Assurance Architecture

Specimen Paper – This is not a complete sample paper.

Attempt all 85 multiple-choice questions – 1 mark awarded to each question. Mark only one answer to each question. There are no trick questions.

Section A – multiple-choice questions
There are 60 questions for Section A, awarding 1 mark per question for a total of 60 points.

Section B – Scenario based multi-choice questions
There are 25 questions for Section B, over 5 scenarios, awarding 13 points per scenario, for a total of 65 points.

Pass Mark: 81/125 65%

This specimen paper has 30 questions in Section A with 30 points available for Section A and 3 scenarios with 15 questions in Section B with 39 points available. Therefore there are 69 points available for both sections.

Specimen Paper Pass Mark: 45/69 65%

Copying of this paper is expressly forbidden without the direct approval of BCS, The Chartered Institute for IT.

Section A
Multiple-choice answers – 1 mark each
NOTE: Choose only one answer per question

1 What is the correct ordering (Conceptual to Component) of the following artefacts for the SABSA Motivation (WHY) foci?

a. Security Policies.
b. Security Standards.
c**.** Control Objectives.
d**.** Security Rules, Practices and Procedures.

A c, a, d and b.
B a, c, b and d.
C b, a, d and c.
D c, b, a and d.

2 In the TOGAF Content MetaModel, under which viewpoint would you find the Business Principles, Objectives and Drivers?

A Motivation.
B Architecture Realisation.
C Architecture Vision.
D Preliminary.

3 Which of the following is **NOT** a responsibility of a Security Architect (rather than Senior or Lead Architect) as defined by CESG?

A Understand the business environment.
B Identify information risks that arise from potential solutions.
C Propose alternative architectures or countermeasures.
D Assist with the secure configuration of ICT systems.

4 Removing version numbers from information given out by an application is an example of which design principle?

A Promote Privacy.
B Limit Enumeration.
C Fail Securely.
D Service Minimisation.

5 Which of the following design principles applies equally to physical and procedural controls as well as technical controls?

A Retrofitting Security is Hard.
B Defence in Depth.
C Psychological Acceptability.
D Segregation of Duties.

6 Why is a large ‘key space’ important in cryptography?

A It makes brute force attacks less feasible.
B It makes the algorithm stronger.
C It makes the cryptanalysis more complex.
D It provides larger randomness in ciphertext output.

7 Which of the following countermeasures allow you to recover from the threat of tampering?

A Backup.
B Intrusion Detection Systems (IDS).
C Authentication.
D Encryption.

8 What is vulnerability?

A A defect that has an adverse effect on the security of the system.
B A potential occurrence that can have an adverse effect.
C The level of threat that a system is exposed to.
D A weakness of an asset, or control that can be exploited by one or more threats.

9 How is a SQL Injection attack delivered?

A An Administrator uploads rogue SQL code.
B A User is tricked into running a SQL script.
C A SQL code fragment is provided instead of a valid input.
D A website is tricked into hosting a SQL script.

10 Which of the following is **NOT** a class of attributes defined in the NIST ABAC model?

A Object.
B Subject.
C Resource.
D Environment.

11 What is the attack surface?

A The collection of devices that have not been hardened.
B The collection of vulnerabilities in the system.
C The services that are exposed to an End User.
D All of the differ points where an attacker could get into a system, and where they could get data out.

12 What is the correct definition of a threat?

A The exploitation of a vulnerability to have an adverse effect on the assets and resources associated with the system.
B The potential occurrence, malicious or otherwise, that can have an adverse effect on the assets and resources associated with the system.
C A characteristic that makes it possible for an attack to occur.
D The risk that a threat actor will take an action which will compromise the integrity of the system.

13 Which of the following is **NOT** a security benefit of application virtualisation?

A Easier packaging.
B Limits access to the underlying OS.
C Easier management of devices.
D Streamlined patching.

14 What is the **MAIN** advantage of the SDL Threat Modelling Tool?

A It can be run on any system level model, irrespective of modelling language.
B It automatically identifies the impact of the threats to a system allowing the Security Architect to focus on the mitigations.
C It provides a systematic way of recording the threats, impacts and mitigations for a system.
D It is an easy to use tool that can be used by IT Professional as well as Security Architects.

15 What is the relationship between an Access Control List (ACL) and an Access Control Entry (ACE)?

A An Access Control List compromises of one or more Access Control Entries.
B An Access Control List contains the set of permissions and the Access Control entry is a log file event for successful access.
C An Access Control List contains Users whereas the Access Control Entry contains the permissions.
D An Access Control List contains the permissions and the Access Control Entry makes the access decision.

16 In cryptology, what is ‘security association’?

A The information that describes how communicating entities provide security.
B The perceived level of security provided by cryptography.
C The differences between the actual and perceived level of security provided by cryptography.
D A group of like-minded entities to enhance security within their organisation.

17 Which of the following is **NOT** one of the 12 PCI DSS requirements?

A Develop and maintain secure systems and applications.
B Install and maintain a firewall configuration to protect cardholder data.
C Protect stored cardholder data.
D Determine Governance and Security Approaches.

18 Which of the following are required for successful Information Assurance (IA) management?

a. Policies.
b. Penetration testing.
c. Procedures.
d. Standards.
e. ISO27001.
f. Toolsets.
g. Common vocabulary.

A a, c, d, f and g.
B a, b, d, f and g.
C b, d, e, f and g.
D a, b, c, d, e, f and g.

19 What is the UK evaluation scheme that helps private sector companies develop cryptographic products?

A Federal Information Processing Standards Publication (FIPS).
B Commercial Product Assurance (CPA).
C CESG Assisted Products Service (CAPS).
D Information Technology Security Evaluation and Certification Scheme (ITSEC).

20 Which of the following is **NOT** a component of Compliance?

A Regulations.
B Security requirements.
C Contracts.
D Strategies and policies.

21 Which of the following is an international IT Service Management (ITSM) Standard?

A ISO 9000.
B ISO 20000.
C ISO 27001.
D ISO 14000.

22 Which of the following are FIPS approved algorithms?

a. Triple Data Encryption Standard (Triple DES).
b. Advanced Encryption Standard (AES).
c. Data Encryption Standard (DES).
d. Digital Signature Standard (DSS).
e. Hashing functions: SHA1, SHA224, SHA384, SHA512.
f. Rivest Cipher 4 (RC4).
g. RSA Signatory Algorithm.

A a, b, d, e and g.
B a, b, c, e, and g.
C a, b, d, e, f and g.
D b, c, d, f and g.

23 Which of these tools are you **MOST LIKELY** to use during the Discovery phase of a Penetration test?

A Nessus.
B Wireshark.
C Network Mapper (Nmap).
D Burp.

24 What is described by NIST as “The security status of an organisation’s networks, information and systems based on IA resources (e.g people, hardware, software, policies) and capabilities in place to manage the defence of the organisation and to react as the situation changes?

A Security Culture.
B Security Policy.
C Security Risk.
D Security Posture.

25 Which of the following is **NOT** a team role when planning a Change Roadmap?

A Sponsor.
B Quality manager.
C Project leader.
D Change agents.

26 Which role in the organisation is responsible for Information security and assurance, compliance and risk management, Cybersecurity, CERT/CSIRT, Security Architecture and Disaster recovery?

A Senior Information Risk Owner (SIRO).
B Departmental Security Officer (DSO).
C Accreditor.
D Chief Information Security Officer (CISO).

27 The IA Maturity Model (IAMM) created by the UK’s National Technical Authority for Information Assurance, CESG, is aligned with which international standard?

A ISO 27001.
B ISO 14000.
C ISO 27005.
D ISO 31000.

28 Which attacks involves tricking the user into inadvertently issuing an HTTP request to a website without their knowledge, usually with malicious intent?

A Application-Layer Attack.
B Cross Site Scripting (XSS).
C Denial-of-Service Attack (DOS).
D Cross Site Request Forgery (CSRF).

29 Which type of testing ensures that a system can gracefully handle invalid input or unexpected user behaviour?

A Positive testing.
B Negative testing.
C SQL injection.
D Vulnerability testing.

30 Which of the following are dependencies necessary for the Implementation phase of the development lifecycle?

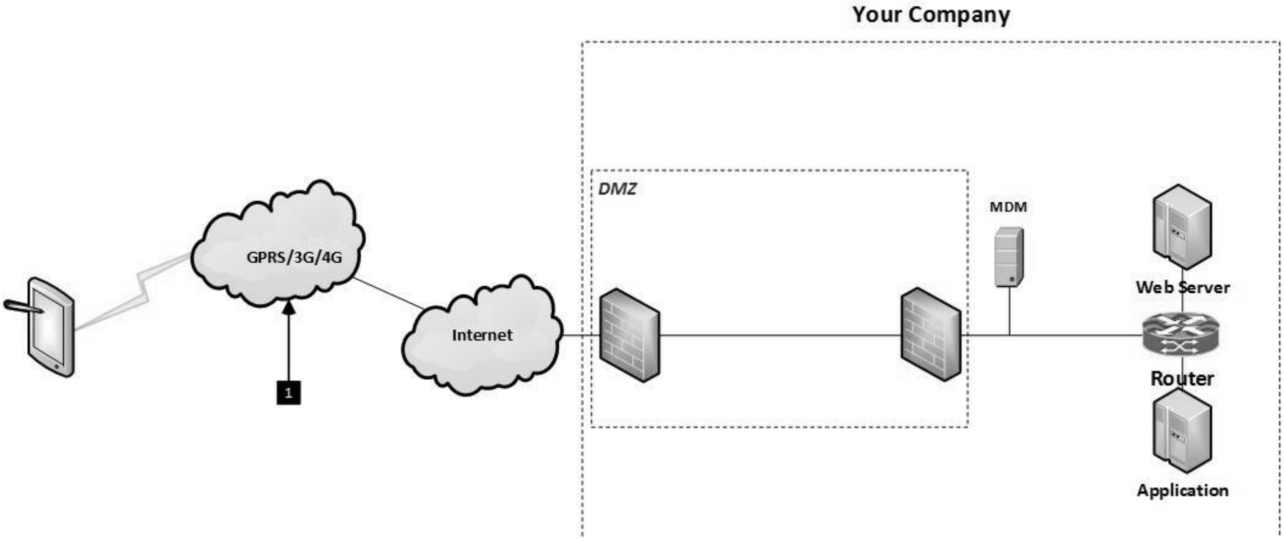
a. System design.
b. Security requirements.
c. Threat model.
d. Terms of reference.
e. Products.

A a, c, and e.
B a, b, c, d and e.
C c, d and e.
D b only.

Section B
Multiple-choice answers – 1 mark each
NOTE: Indicate which of the following answers apply.

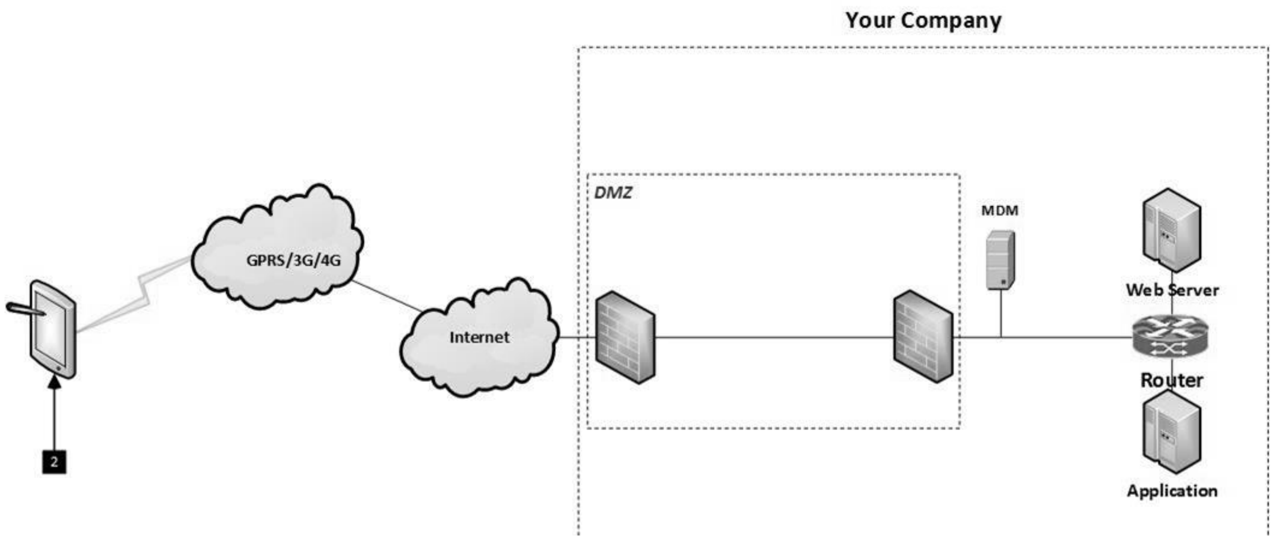
Scenario 1

Your company conducts 'mystery shopper' visits to client's stores in order to improve customer service. The company is thinking of replacing the existing paper-based reporting system with a website to allow workers to input the results of their visit and provide up to date results to their clients. They are considering whether to issue everyone with a company tablet or start a Bring Your Own Device (BYOD) scheme.



31 What are the **PRIMARY** threats across the mobile bearer (indicated by position 1 in the figure)? Select all that apply.

A Tampering.
B Information Disclosure.
C Repudiation.
D Denial of Service.
E Elevation of Privilege.

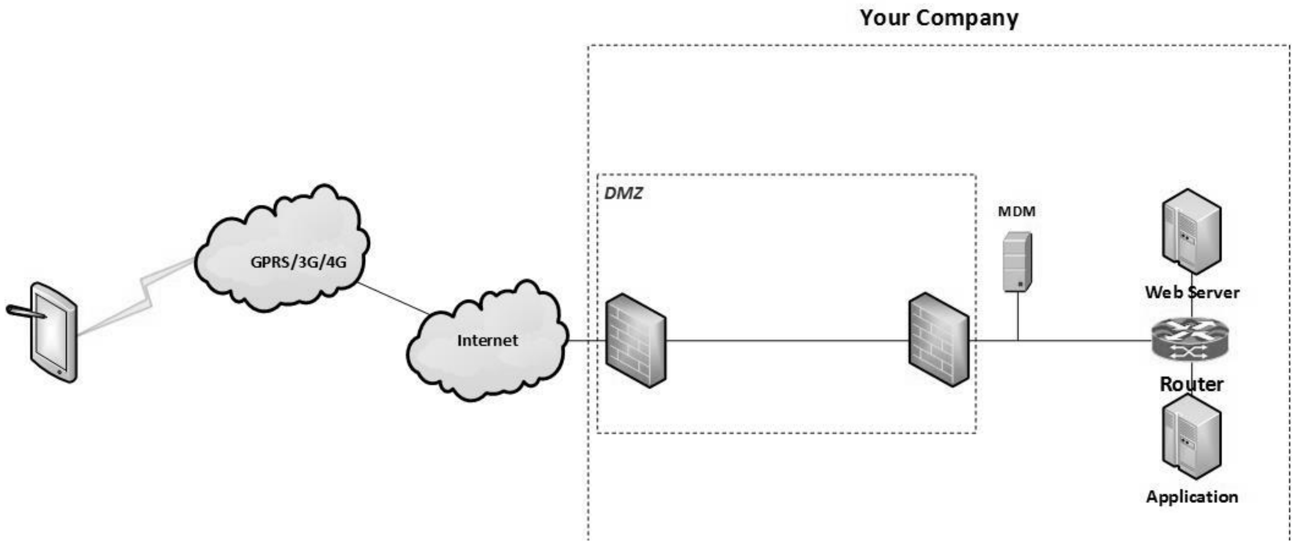


32 What technologies **COULD** you use on the Mobile Device (indicated by position 2 in the figure) to mitigate the threat of Tampering? Select all that apply.

A VPN.
B TLS.
C Virtualised Applications.
D SAML.
E HIPS.

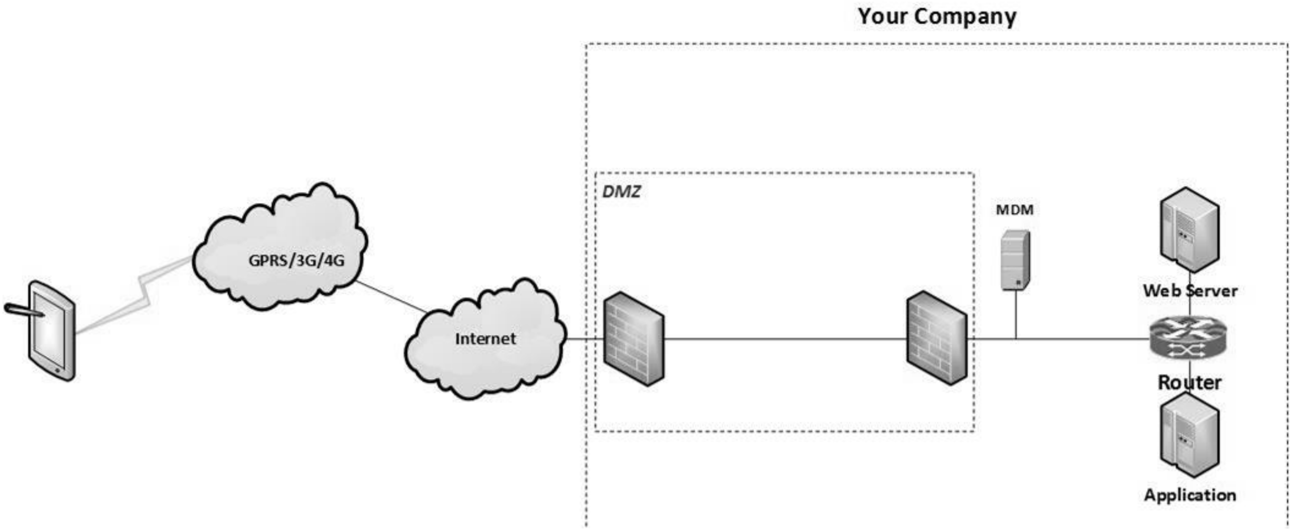
33 What are the primary concerns with a BYOD scheme compared to company tablets? Select all that apply.

A Limiting access to authorised devices.
B Loss / theft of the device.
C Separation of personal and business data.
D Timely application of security patches.
E Consistency of security controls.



34 What controls **COULD** be implemented to limit the amount of business information stored on a personal device? Select all that apply.

A Limiting access to only mobile workers.
B Use of container management to separate personal and business data.
C Encryption of business data on the personal device.
D Limiting ability to download through file type / size enforcement.
E Use of sandboxing for virtual applications.

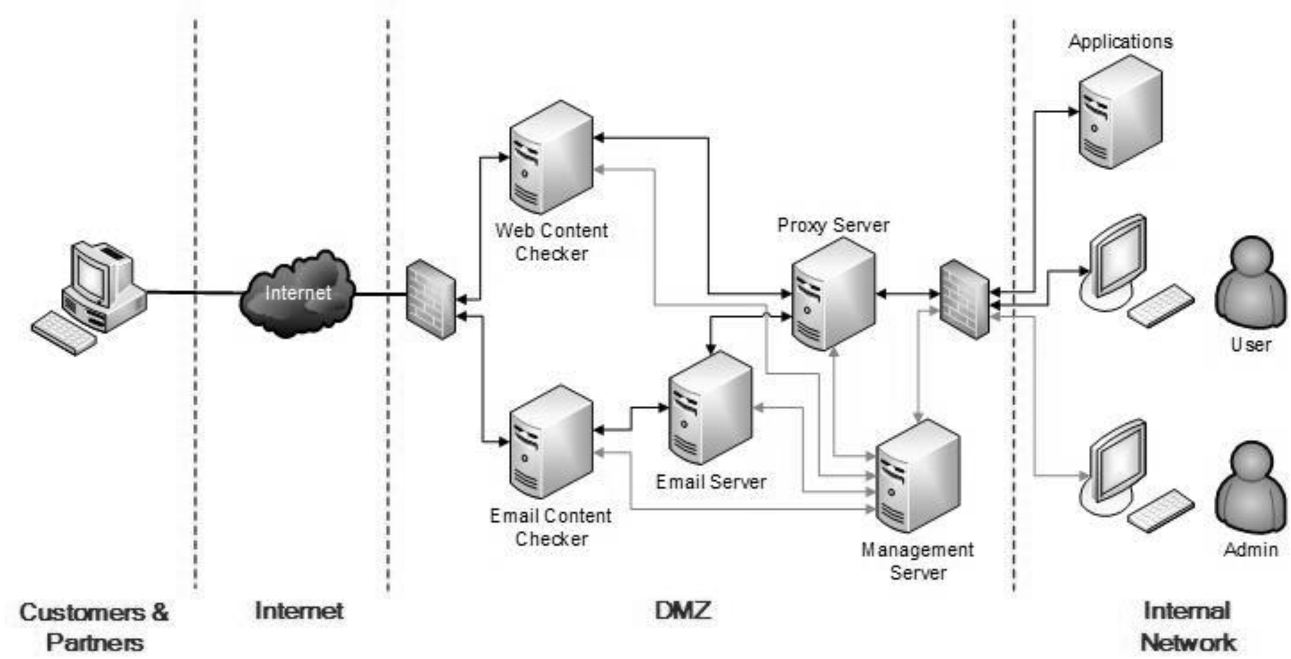


35 What controls would you expect to see in the DMZ to protect against rogue Users? Select all that apply.

A Strong authentication.
B Content scanning.
C Limited access to applications.
D Virtualisation.
E Remote administration.

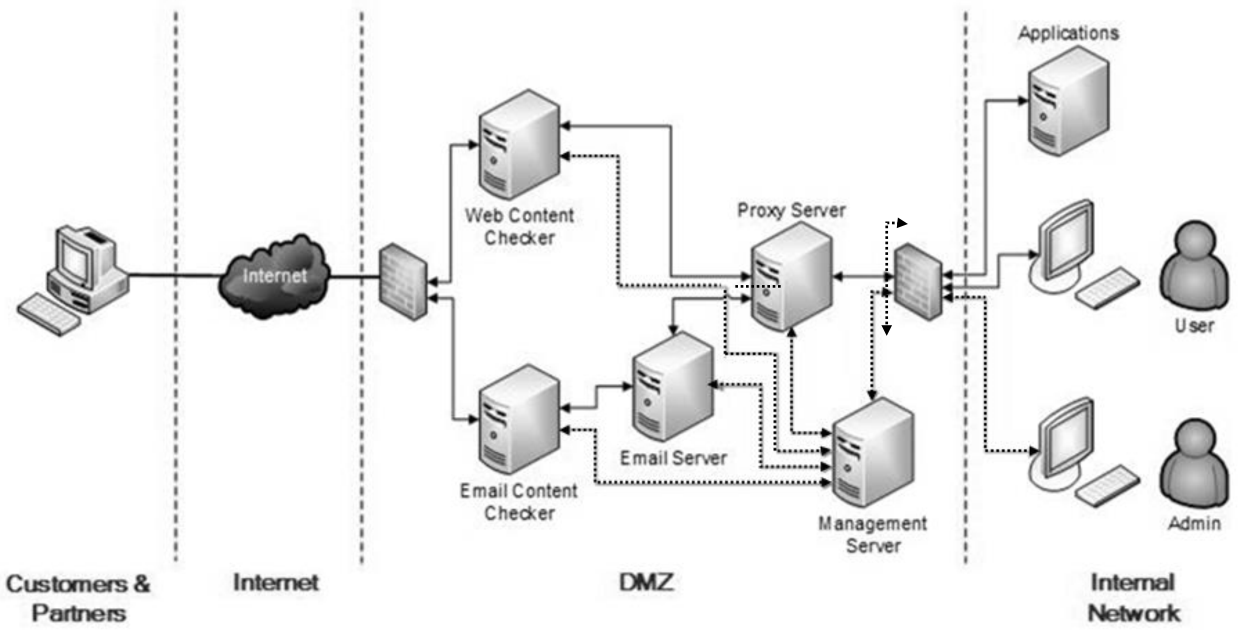
Scenario 2

Your company has recently suffered from a cyber-attack which caused £500,000 in lost productivity and downtime. They have decided to implement a DMZ to control the communication channels out of the company. They foresee the need to protect themselves from malicious content from the internet as well as enforcing company policy on releasing material.



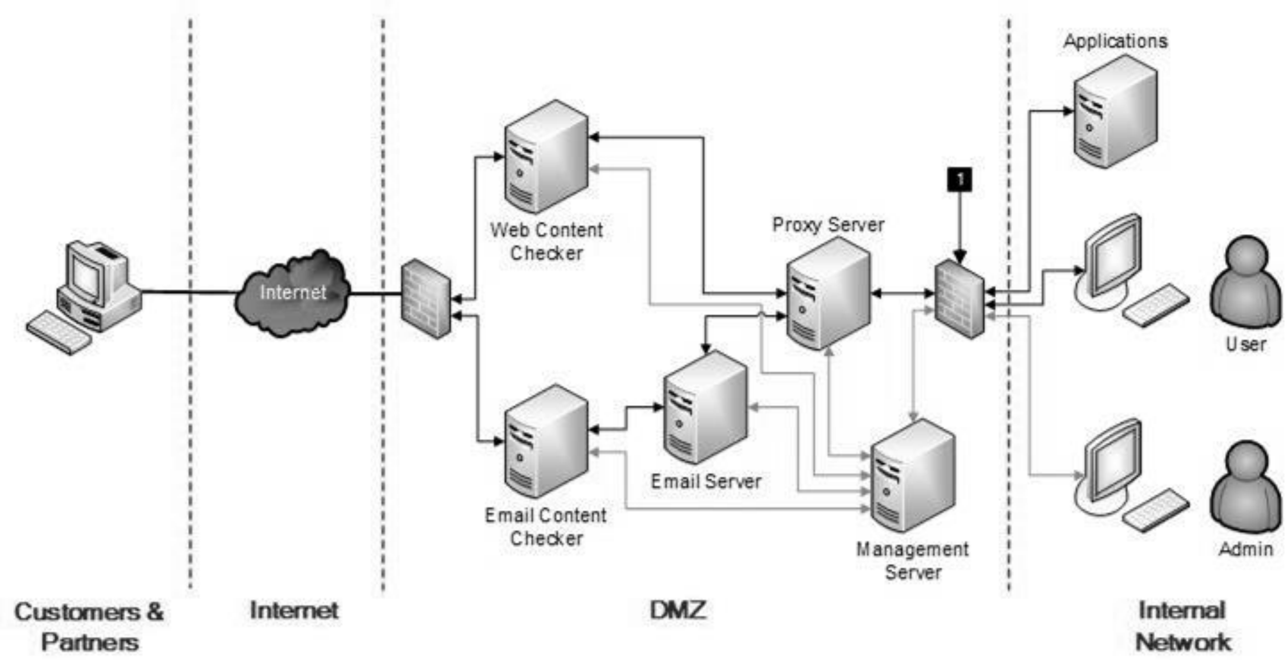
36 You have recommended adding a management server to the DMZ design. What functions **COULD** this provide? Select **all** that apply.

A Patching (including AV signatures).
B Audit collection.
C System monitoring.
D Traffic inspection.
E Application configuration.



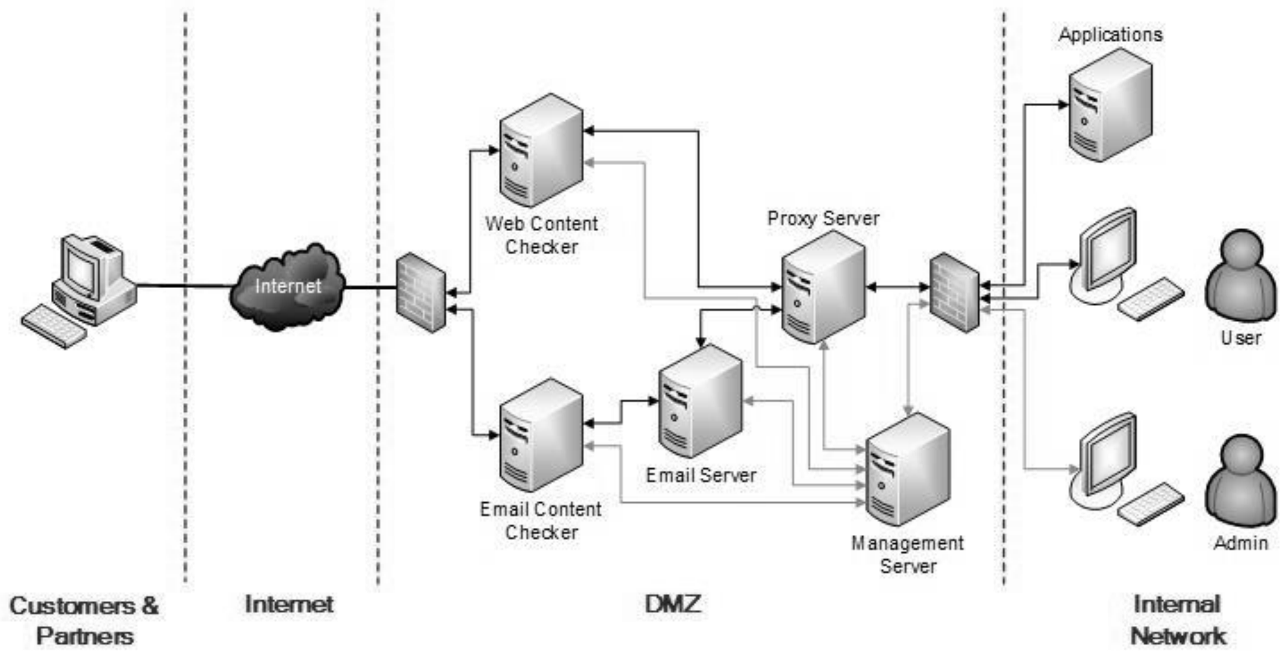
37 How **COULD** you prevent the management traffic (shown using a dotted line in the figure) from being tampered with by ordinary Users? Select all that apply.

A Limit access to the management console.
B Change the ports used for management traffic.
C Encrypt the management traffic.
D Auditing of the management traffic.
E Segregate the traffic onto separate VLANs.



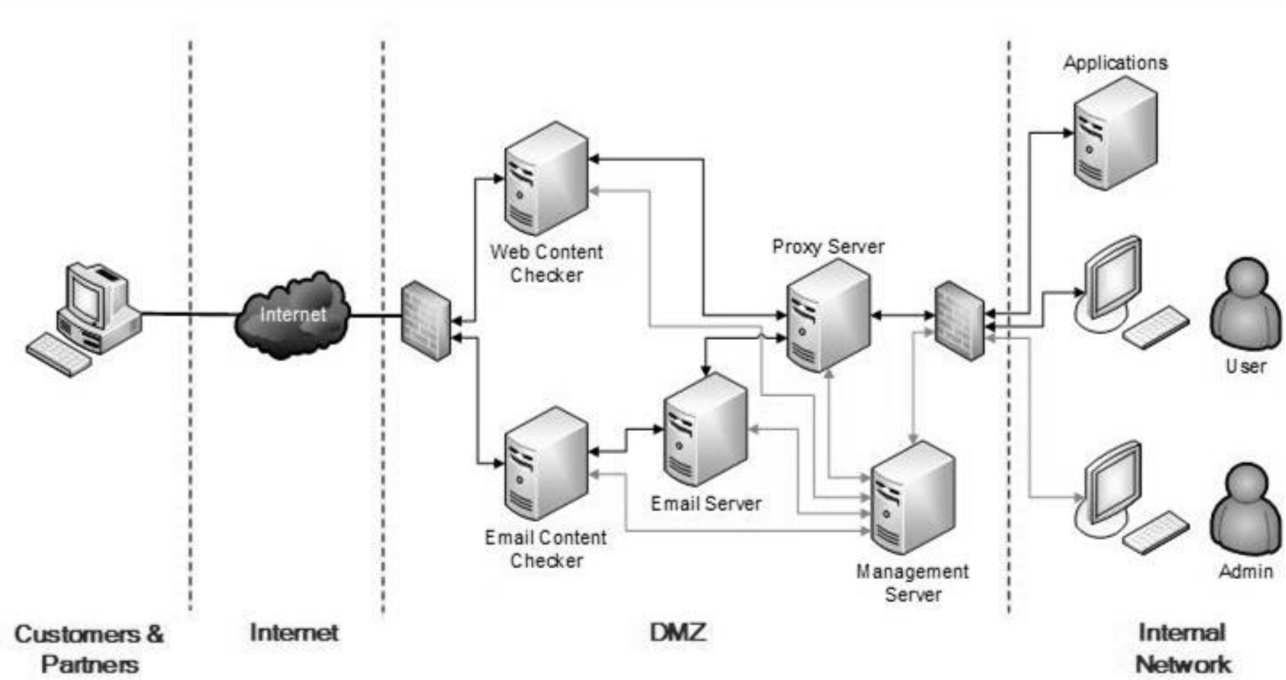
38 What controls **COULD** you implement on the internal firewall (indicated by position 1 on the figure) to protect the internal network in the event that the DMZ is compromised? Select **all** that apply.

A Limit access to IP addresses based on source.
B Limit traffic to specified applications.
C Monitor audit logs.
D Block all incoming traffic.
E Authenticate servers.



39 What controls **COULD** you implement on the proxy to limit the company's exposure to malicious content on the internet? Select all that apply.

A Whitelist URLs.
B Block self-signed certificates for SSL/TLS.
C Authenticate customers using Kerberos.
D Enable SSL 2.0.
E Validate addresses against an internet-based DNS service.

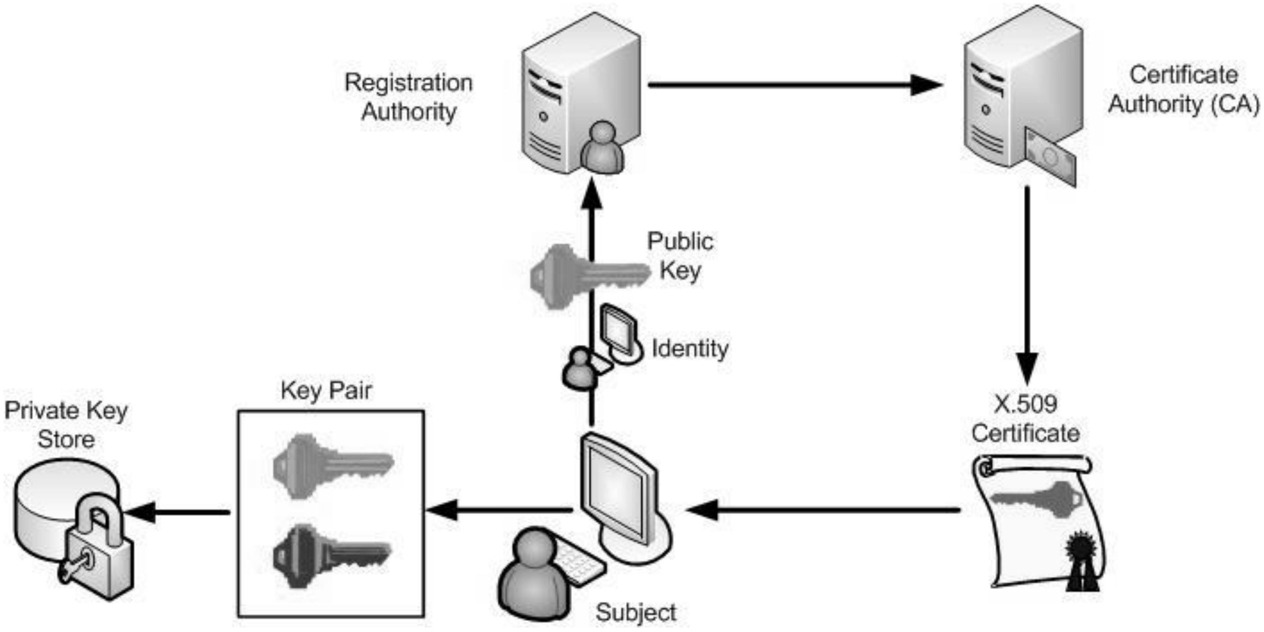


40 What threats does the Administrator pose if they have the equivalent of local administrator access to all servers in the DMZ? Select all that apply.

A Misconfiguration of services.
B Stopping services.
C Deletion of audit logs.
D Elevating others to Administrator.
E Modifying network routing.

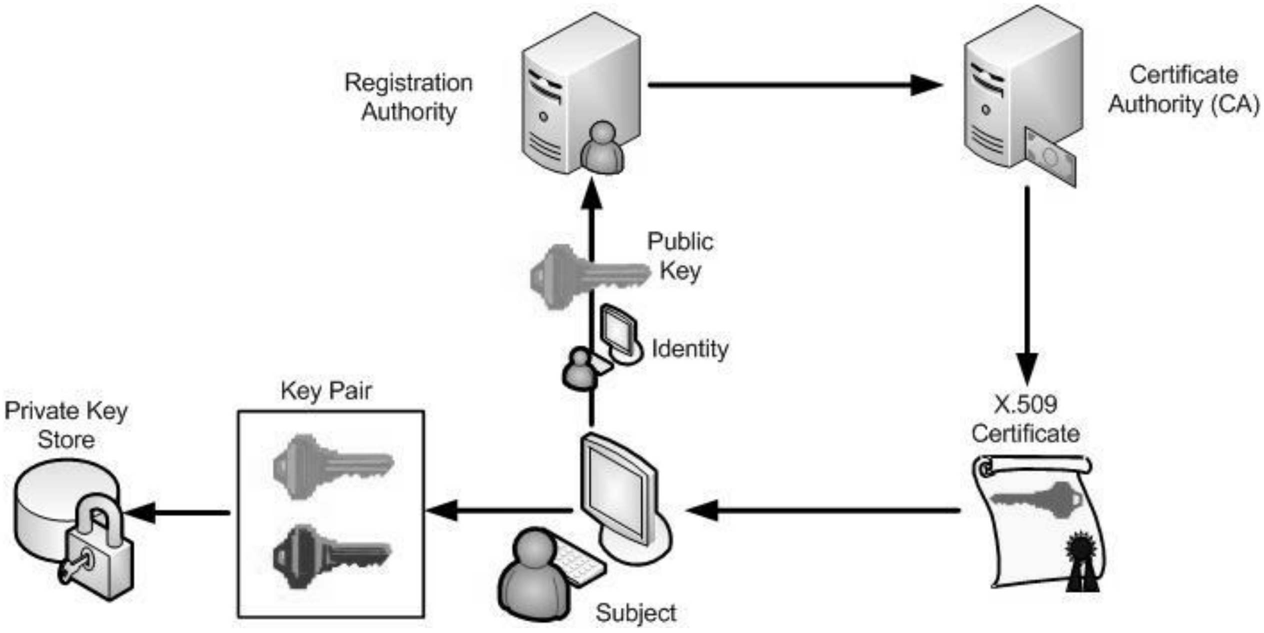
Scenario 3

Your company is implementing a Public Key Infrastructure (PKI) such that you can control access to the network using 802.1x authentication, approve and authorise applications with Code Signing, implement two-factor authentication using Smart Cards and protect traffic to internal web-sites with SSL. Your proposed certificate request process is shown in the diagram.



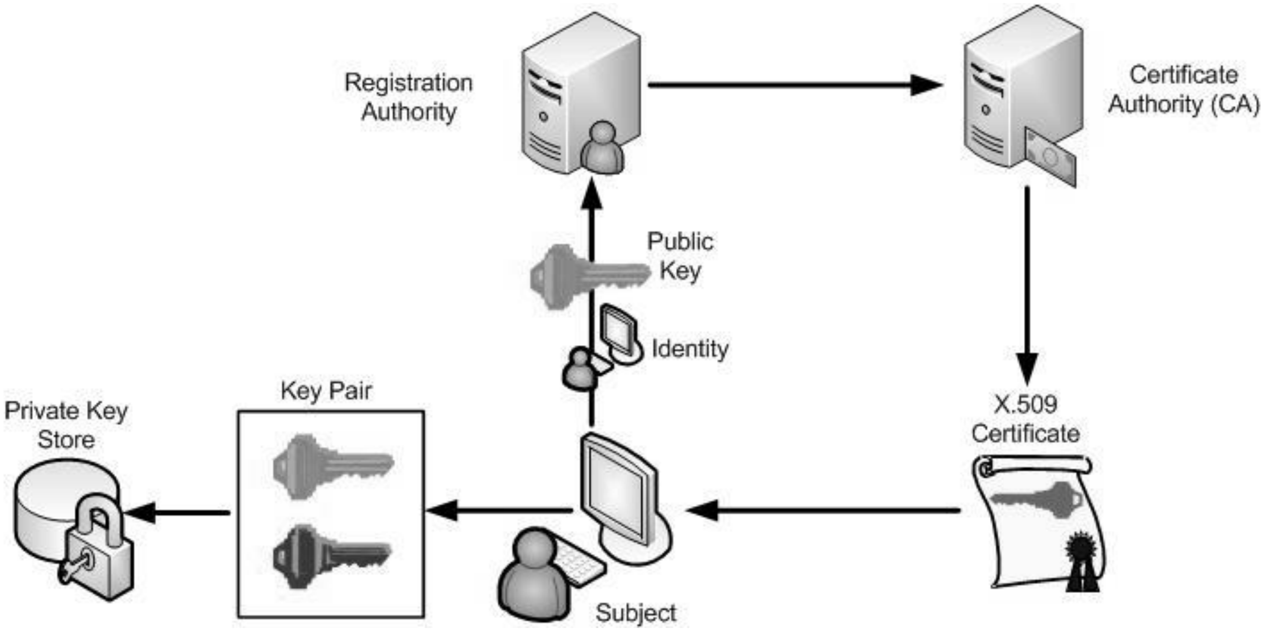
41 What is the role of the Certificate Authority? Select all that apply.

A It must be assured by an offline root CA.
B The public key must be RSA 2048 bits.
C Maintains and issues the Certificate Revocation List (CRL).
D An entity that issues digital certificates.
E Allows others (relying parties) to rely upon signatures or assertions made by the owner of the private key.



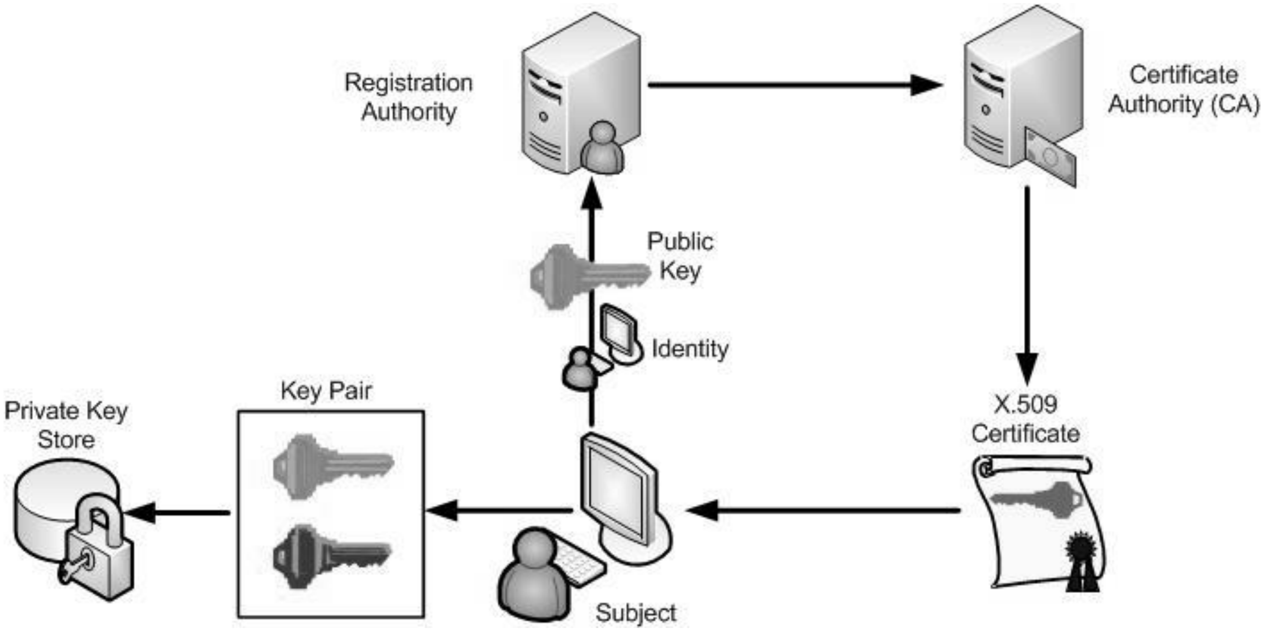
42 Which fields would you expect to find in the X.509 certificate structure purchased from the CA? Select all that apply.

A Fingerprint.
B Signature hash algorithm.
C Serial number.
D CRL.
E Private key.



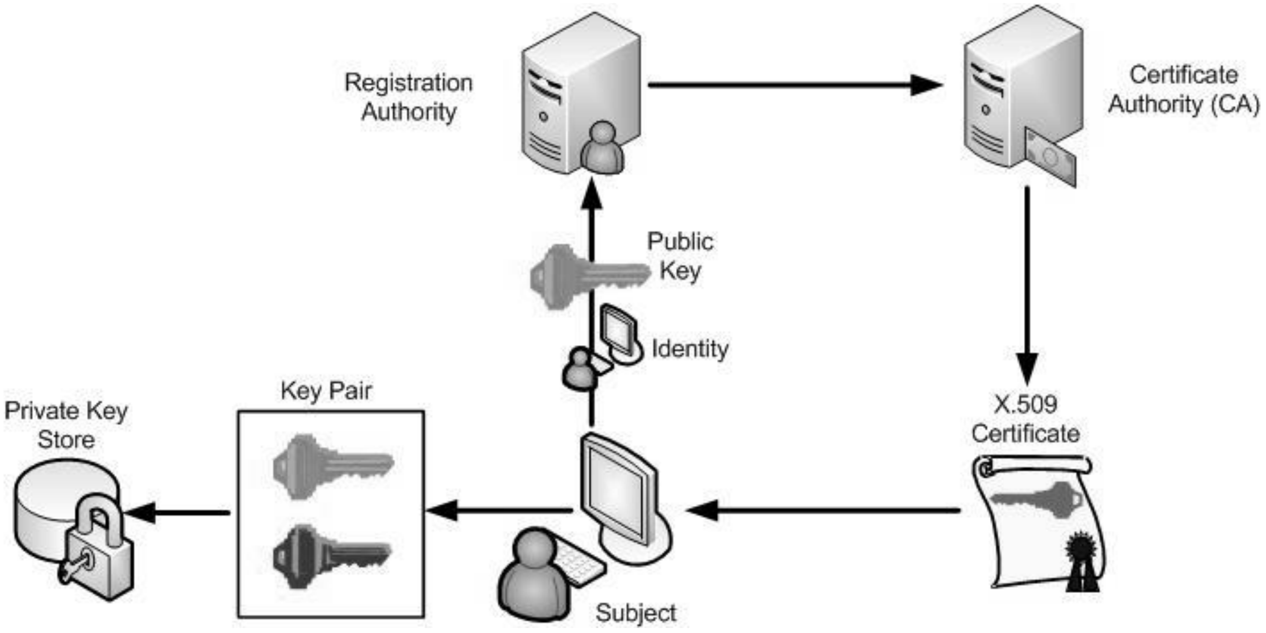
43 Which of the following threats would you be addressing by providing a secure connection to your business's website? Select all that apply.

A Denial of Service.
B Spoofing.
C Information disclosure.
D Tampering.
E DNS poisoning.



44 What are the threats associated with the certificate validity period? Select all that apply.

A Long certificate validity periods cannot be used with smart cards.
B The longer the certificate validity period the more feasible a brute force attack on the private key.
C The longer the certificate validity period the more processing power is required.
D Short certificate validity periods are associated with self-signed certificates.
E Short validity periods require more certificate re-issues and consequently higher system disruption potential.



45 Which of the following would be a suitable location for the private key store? Select all that apply.

A NTFS file store.
B C:\Users\%Username%\Certificates.
C Java key-store.
D Hardware Security Module (HSM).
E Smart Card.

-End of Paper-