

CONTOSO

1.

What is CL's tolerance for risk? (Choose one)

- A. CL is willing to try some new approaches.
- B. CL is comfortable with a high level of risk.
- C. CL is willing to risk the entire company for large rewards.
- D. CL is willing to try only those approaches that they have successfully implemented before.
- E. CL is very conservative and does not take any chances.

2.

What is the primary security risk for the desktop computers at CL? (Choose one)

- A. Another CL employee connected to a desktop computer via the LAN.
- B. Denial-of-service attack launched from the internet targeting a desktop computer.
- C. Remote hackers directly connected to a desktop computer via the internet.
- D. Remote hackers directly connected to a desktop computer via modem.

3.

Design an authentication strategy for the web site after certificates have been issued to the brokers.

Use only computers and authentication methods that apply.

Computer Authentication method

- A. Kerberos
- B. Basic authentication with SSL
- C. SSL and directory services (DS) mapping
- D. HTTP and directory services (DS) mapping

- 1. Broker
- 2. CONTDC
- 3. CONTDATA
- 4. CONTWEB1
- 5. CONTVPN
- 6. CL

SSL and DS SSL and DS

Broker----| |--CONTWEB1---| |---CL

Answer: 1 > C > 4 > A > 2 > 3

4.

How should you design the active directory structure for CL? (Choose one)

- A. Create a single domain in its own forest. Do not establish trust relationships.
- B. Create a single domain in its own forest. Establish a one-way trust relationship with Adatum
- C. Create one child domain. Place the child domain in the same forest as AD's domain tree.
- D. Create one domain in its own domain tree. Place the domain tree within the same forest as AD's domain tree.

5.

Which three options should you include in a security template for CONTWEB1? (Choose three)

- A. Rename the administrator account.
- B. Allow CD-ROM access to all users.

- C. Limit CD-ROM access to users who are logged on locally.
- D. Enforce strong passwords.
- E. Set the NTLM authentication level to LM and NTLM.
- F. Disable account lockout.

6.

Which technology or technologies should you implement to provide the highest level of security for communications between employees of AD and CL? (Choose one)

- A. Internet authentication services (IAS) and NTLM authentication.
- B. PPTPC, SSL, digital certificates, and directory services (DS) mapping.
- D. Basic authentication with SSL.
- E. L2TP over IPsec

7.

How should you separate intranet resources from publicly visible internet servers? (Choose one)

- A. Use a private IP address space. Configure both the internal DNS and the authoritative internet based DNS server to resolve both internal and external names.
- B. Use corp.contoso.com as a suffix for all internal sites. Configure both the internal DNS and the authoritative internet based DNS server to resolve both internal and external names.
- C. Use corp.contoso.com as a suffix for all internal sites. Configure the internal DNS to resolve internal names, but do not include these names in the authoritative internet based DNS server.
- D. Use a private IP address space. Configure the authoritative internet based DNS server to resolve internal names, but do not include these names on the internal DNS server.

8.

Which technology or technologies should you include in your security strategy to secure broker access to the web site? (Choose one)

- A. Basic authentication with SSL.
- B. SSL, digital certificates, and directory services (DS) mapping.
- C. Internet authentication services (IAS) and an ODBC database.
- D. L2TP over IPsec

9.

How should you implement a Public Key Infrastructure (PKI) for CL? (Choose one)

- A. Install an online enterprise root CA. Install an online enterprise subordinate CA. Import a self signed server certificate on the subordinate CA. Issue client certificates on the subordinate CA.
- B. Install an offline stand alone root CA. Install an online stand alone subordinate CA. Issue client certificates on the root CA.
- C. Install an online stand alone root CA. Import a server certificate from a third party CA to the root CA certificate trust list. Use client certificates from third party CA.
- D. Install an offline enterprise root CA. Install an online enterprise subordinate CA. Issue client certificates on the subordinate CA.

10.

What should you include in an audit policy for CONTDC? (Choose all that apply)

- A. Success and failure audit for object access.
- B. Success and failure audit for directory services access.
- C. Success and failure audit for policy change.
- D. Success and failure audit for account management.
- E. Success and failure audit for account logon events.