Cybersecurity Maturity Model Certification (CMMC) is a framework developed by the U.S. Department of Defense (DoD) to enhance cybersecurity practices across the Defense Industrial Base (DIB). CMMC Level 1 is the entry point into this framework and is designed to ensure that basic cyber hygiene practices are followed by contractors who handle Federal Contract Information (FCI).

This document provides a comprehensive overview of CMMC Level 1, covering the structure, practices, assessment methods, and practical implementation considerations, without any duplication.

CMMC Level 1 comprises 17 practices across six key domains. These practices are derived from the Federal Acquisition Regulation (FAR) clause 52.204-21 and do not require process maturity or documentation beyond evidence of implementation.

1. Access Control (AC)
2. Identification and Authentication (IA)
3. Media Protection (MP)
4. Physical Protection (PE)
5. System and Communications Protection (SC)
6. System and Informatio
n Integrity (SI)

Access Control (AC):

- AC.1.001: Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems). This ensures that only legitimate users gain access to sensitive data.

- AC.1.002: Limit information system access to the types of transactions and functions that authorized users are permitted to execute. Role-based access must be enforced.
- AC.1.003: Verify and control/limit connections to and use of external information systems. This includes restricting connections to untrusted networks.
- AC.1.004: Control information posted or processed on publicly accessible information systems. Sensitive or contract-relevant content should never be published externally.

Identification and Authentication (IA):

- IA.1.076: Identify information system users, processes acting on behalf of users, or devices. Unique identification helps track and control system use.
- IA.1.077: Authenticate (or verif
y) the identities of those users, processes, or devices. Authentication mechanisms may include passwords, multi-factor authentication, and certificates.

Media Protection (MP):

- MP.1.118: Sanitize or destroy information system media containing FCI before disposal or release for reuse. This prevents unauthorized recovery of sensitive data.

Physical Protection (PE):

- PE.1.131: Limit physical access to organizational systems, equipment, and operating environments to authorized individuals.
- PE.1.132: Escort visitors and monitor visitor activity. This includes sign-in logs and physical supervision.
- PE.1.133: Maintain audit logs of physical access. This can include badge logs or manual logs for data centers.
- PE.1.134: Control and manage physical access devices. This includes badges, keys, and biometric devices.

System and Communications Protection (SC):

- SC.1.175: Monitor, control, and protect organizational communications (e.g., information transmitted or received) at the externa

l boundaries and key internal boundaries of the information systems.

- SC.1.176: Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

System and Information Integrity (SI):

- SI.1.210: Identify, report, and correct information and information system flaws in a timely manner. Patch management practices fall under this control.

- SI.1.211: Provide protection from malicious code. Antivirus and endpoint detection systems help meet this requirement.

- SI.1.212: Update malicious code protection mechanisms when new releases are available. This includes signature updates and engine upgrades.

- SI.1.213: Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

Implementation Tip for Practice 1: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures

, logs, or access control lists as evidence.

Implementation Tip for Practice 2: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 3: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control

lists as evidence.

Implementation Tip for Practice 4: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 5: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 6: Ensure policy enforcement, training, and loggin
g mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 7: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 8: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 9: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 10: Ensure policy enforcement, training, and logging mechanisms

are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as ev

idence.

Implementation Tip for Practice 11: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 12: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 13: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 14: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 15: Ensure policy enforcement, training, and logging mechanisms are in place to dem

onstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 16: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access

control lists as evidence.

Implementation Tip for Practice 17: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 18: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 19: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip f

or Practice 20: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 21: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 22: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 23: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 24: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during au

dits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 25: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 26: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 27: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 28: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 29: Ensure policy

enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 30: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 31: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 32: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 33: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures
, logs, or access control lists as evidence.

Implementation Tip for Practice 34: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 35: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 36: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access

control lists as evidence.

Implementation Tip for Practice 37: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 38: Ensure policy enforcement, training, and l
ogging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 39: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 40: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 41: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 42: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lis
ts as evidence.

Implementation Tip for Practice 43: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 44: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 45: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 46: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 47: Ensure policy enforcement, training, and logging mechanisms are in plac
e to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 48: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 49: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access

control lists as evidence.

Implementation Tip for Practice 50: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 51: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementati
on Tip for Practice 52: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 53: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 54: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 55: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 56: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance d

uring audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 57: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 58: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 59: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 60: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 61: Ensur

e policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 62: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 63: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 64: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 65: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen
captures, logs, or access control lists as evidence.

Implementation Tip for Practice 66: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 67: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 68: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 69: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access

control lists as evidence.

Implementation Tip for Practice 70: Ensure policy enforcement, trainin
g, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 71: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 72: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 73: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 74: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access con
trol lists as evidence.

Implementation Tip for Practice 75: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 76: Ensure policy enforcement, training, and logging mechanisms

are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 77: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 78: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 79: Ensure policy enforcement, training, and logging mechanisms are

in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 80: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 81: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 82: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 83: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Impl

ementation Tip for Practice 84: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 85: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 86: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 87: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 88: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate comp

liance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 89: Ensure policy enforcement, training, and logging mechanisms

are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 90: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 91: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 92: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 9
3: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 94: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 95: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 96: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 97: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide
screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 98: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 99: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 100: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 101: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 102: Ensure policy enforceme
nt, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 103: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 104: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 105: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 106: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs
, or access control lists as evidence.

Implementation Tip for Practice 107: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 108: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 109: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access

control lists as evidence.

Implementation Tip for Practice 110: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 111: Ensure policy enforcement, training, and lo
gging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 112: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 113: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 114: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 115: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control
lists as evidence.

Implementation Tip for Practice 116: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 117: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 118: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 119: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 120: Ensure policy enforcement, training, and logging mechanisms are

in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 121: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 122: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access

control lists as evidence.

Implementation Tip for Practice 123: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 124: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 125: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 126: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 127: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 128: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 129: Ensure policy enforcement, training, and logging mechanisms

are in place to demonst

rate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 130: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 131: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 132: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 133: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip f

or Practice 134: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 135: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 136: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 137: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 138: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance duri
ng audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 139: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 140: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 141: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 142: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access

control lists as evidence.

Implementation Tip for Practice 143: Ens

ure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 144: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 145: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 146: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 147: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide s

creen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 148: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 149: Ensure policy enforcement, training, and logging mechanisms

are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 150: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 151: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 152: Ensure policy enforceme
nt, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 153: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 154: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 155: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 156: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs
, or access control lists as evidence.

Implementation Tip for Practice 157: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 158: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 159: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 160: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 161: Ensure policy enforcement, training, and lo
gging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 162: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 163: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 164: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 165: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control
lists as evidence.

Implementation Tip for Practice 166: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 167: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 168: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 169: Ensure policy enforcement, training, and logging mechanisms

are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 170: Ensure policy enforcement, training, and logging mechanisms are

in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 171: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 172: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 173: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 174: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 175: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 176: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 177: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 178: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 179: Ensure policy enforcement, training, and logging mechanisms are in place to demonst
rate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 180: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 181: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 182: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access

control lists as evidence.

Implementation Tip for Practice 183: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip f

or Practice 184: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 185: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 186: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 187: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 188: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance duri

ng audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 189: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 190: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 191: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 192: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 193: Ens
ure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 194: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 195: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 196: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 197: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide s
creen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 198: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 199: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 200: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 201: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 202: Ensure policy enforceme
nt, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide

screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 203: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 204: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 205: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 206: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs
, or access control lists as evidence.

Implementation Tip for Practice 207: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 208: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 209: Ensure policy enforcement, training, and logging mechanisms

are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 210: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 211: Ensure policy enforcement, training, and lo
gging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 212: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 213: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 214: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 215: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control
lists as evidence.

Implementation Tip for Practice 216: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 217: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 218: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 219: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 220: Ensure policy enforcement, training, and logging mechanisms are

in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 221: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 222: Ensure policy enforcement, training, and logging mechanisms

are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 223: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 224: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 225: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 226: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 227: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 228: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 229: Ensure policy enforcement, training, and logging mechanisms are in place to demonst

rate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 230: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 231: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 232: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 233: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip f

or Practice 234: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 235: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access

control lists as evidence.

Implementation Tip for Practice 236: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 237: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 238: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance duri
ng audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 239: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 240: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 241: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 242: Ensure policy enforcement, training, and logging mechanisms

are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 243: Ens

ure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 244: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 245: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 246: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 247: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide s

creen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 248: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 249: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 250: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 251: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 252: Ensure policy enforceme
nt, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 253: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 254: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 255: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 256: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs
, or access control lists as evidence.

Implementation Tip for Practice 257: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 258: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 259: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 260: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 261: Ensure policy enforcement, training, and lo
gging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 262: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access

control lists as evidence.

Implementation Tip for Practice 263: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 264: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 265: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control
lists as evidence.

Implementation Tip for Practice 266: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 267: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 268: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 269: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 270: Ensure policy enforcement, training, and logging mechanisms are

in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 271: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 272: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 273: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 274: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 275: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access

control lists as evidence.

Implementation Tip for Practice 276: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 277: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 278: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 279: Ensure policy enforcement, training, and logging mechanisms are in place to demonst
rate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 280: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 281: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 282: Ensure policy enforcement, training, and logging mechanisms

are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 283: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip f

or Practice 284: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 285: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 286: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 287: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 288: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance duri

ng audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 289: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 290: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 291: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 292: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 293: Ens
ure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 294: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 295: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access

control lists as evidence.

Implementation Tip for Practice 296: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 297: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide s
creen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 298: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 299: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Implementation Tip for Practice 300: Ensure policy enforcement, training, and logging mechanisms are in place to demonstrate compliance during audits. Provide screen captures, logs, or access control lists as evidence.

Practice 1 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activit
ies relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 2 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be require

d as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 3 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zon
e (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 4 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 5 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized

identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 6 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs,

screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 7 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization imp

lements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 8 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

P

ractice 9 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials

for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 10 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor auth entication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 11 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may

implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training ma terials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 12 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based crede ntials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled

to prevent unauthorized data transfer.

Practice 13 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 14 Guidance:

Each control must be enforced through both technic

al and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 15 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities
relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 16 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required a

s proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 17 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone
(DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 18 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 19 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized
identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 20 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs,

screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 21 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization i

mplements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 22 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 23 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 24 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor

authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 25 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Trainin
g materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 26 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based c
redentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 27 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 28 Guidance:

Each control must be enforced through both tec

hnical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 29 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may

implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activit

ies relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 30 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be requir

ed as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials.

Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 31 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized z

one (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 32 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 33 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centrali

zed identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 34 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that l

ogs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 35 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organizati

on implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 36 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfe

r.

Practice 37 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor

authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 38 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-fac
tor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 39 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Tra
ining materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 40 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-bas

ed credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 41 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 42 Guidance:

Each control must be enforced through both

technical and procedural means. For example, you may implement a centralized identity provider

for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 43 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all act

ivities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to

prevent unauthorized data transfer.

Practice 44 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be re

quired as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 45 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitariz

ed zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 46 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 47 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a cent

ralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 48 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure th

at logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 49 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organi

zation implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 50 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data tra

nsfer.

Practice 51 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 52 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi
-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 53 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors.

Training materials for staff and change management records may also be required as proof of

ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 54 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role

-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 55 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may

implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 56 Guidance:

Each control must be enforced through

both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to

prevent unauthorized data transfer.

Practice 57 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 58 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also b

e required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 59 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilit

arized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 60 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 61 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a

centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 62 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensur

e that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 63 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An or

ganization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 64 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data

transfer.

Practice 65 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 66 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with m

ulti-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials

for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 67 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for audit

ors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 68 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using
role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 69 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to

prevent unauthorized data transfer.

Practice 70 Guidance:

Each control must be enforced thro

ugh both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 71 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track

all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 72 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may al

so be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 73 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a dem

ilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 74 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 75 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implemen

t a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 76 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

E

nsure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 77 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

A

n organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 78 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized
data transfer.

Practice 79 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials

for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 80 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined wi

th multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 81 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for a

uditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 82 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems us

ing role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 83 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 84 Guidance:

Each control must be enforced

through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 85 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to t

rack all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 86 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records ma

y also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 87 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a

demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 88 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 89 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may impl

ement a centralized identity provider for user authentication, combined with multi-factor

authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 90 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Consideration

s:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 91 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Exampl

e:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 92 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials

for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthori

zed data transfer.

Practice 93 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 94 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combine
d with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 95 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available f
or auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 96 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal system

s using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 97 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 98 Guidance:

Each control must be enfor

ced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 99 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used

to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 100 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management recor

ds may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 101 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolate

d in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 102 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor

authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 103 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 104 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Cons

iderations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 105 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-wo

rld Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 106 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to preven

t unauthorized data transfer.

Practice 107 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 108 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentica

tion, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials.

Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 109 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents a

re available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 110 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to

internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 111 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 112 Guidance:

Each cont

rol must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 113 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanis

ms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 114 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and chang

e management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 115 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor

authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing comp

onents are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 116 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 117 Guidance:

Each control must be enforced through both technical and procedural means.

For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 118 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control

.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 119 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enf

orcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 120 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 121 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials.

Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 122 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider f

or user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 123 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and

policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 124 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restric

ted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 125 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 126 G

uidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 127 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication

. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 128 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may

implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials f or staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 129 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 130 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 131 Guidance:

Each control must be enforced through both technical and

procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials

for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 132 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relev
ant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 133 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as pr

oof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 134 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials.

Public-facing components are isolated in a demilitarized zone (DM

Z). USB ports are disabled to prevent unauthorized data transfer.

Practice 135 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 136 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized i

dentity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 137 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs,

screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 138 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization

implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 139 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 140 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 141 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-fac

tor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 142 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Tr

aining materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 143 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-b
ased credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 144 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 145 Guidance:

Each control must be enforced through

both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 146 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may

implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track al

l activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 147 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also

be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials.

Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 148 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demi

litarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 149 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 150 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may impleme

nt a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 151 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 152 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example

:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 153 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthori

zed data transfer.

Practice 154 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor

authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 155 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combi

ned with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 156 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are availabl

e for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 157 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials

for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal sy

stems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 158 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 159 Guidance:

Each control must be

enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 160 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should b

e used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials.

Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 161 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change managemen

t records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 162 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are

isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 163 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 164 Guidance:

Each control must be enforced through both technical and procedural means. For exampl

e, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 165 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessme

nt Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 166 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 167 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor

authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 168 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 169 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user aut

hentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 170 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy docu

ments are available for auditors. Training materials for staff and change management records may

also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 171 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN acc

ess to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 172 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may

implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 173 Guidance:

Ea

ch control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to

prevent unauthorized data transfer.

Practice 174 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging m

echanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 175 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff an

d change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 176 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-faci

ng components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 177 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 178 Guidance:

Each control must be enforced through both technical and procedural

means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 179 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 180 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor

authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongo

ing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 181 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB por

ts are disabled to prevent unauthorized data transfer.

Practice 182 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 183 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity pro

vider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials

for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 184 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshot

s, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 185 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements

restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 186 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials.

Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practic

e 187 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 188 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authent ication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 189 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training mate
rials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 190 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based creden tials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 191 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 192 Guidance:

Each control must be enforced through both techni

cal and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 193 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activitie

s relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 194 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be require
d as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 195 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized z
one (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 196 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 197 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centra

lized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 198 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may

implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure tha

t logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 199 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organi

zation implements restricted VPN access to internal systems using role-based credentials.

Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 200 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data tr

ansfer.

Practice 201 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 202 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with mu
lti-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 203 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for audit

ors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 204 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 205 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 206 Guidance:

Each control must be enforced t

hrough both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging

mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 207 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to t

rack all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 208 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records m

ay also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 209 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials

for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in

a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 210 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 211 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may

implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 212 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Consider

ations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials.

Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 213 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world

Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 214 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent un

authorized data transfer.

Practice 215 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 216 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication

, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 217 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are a

vailable for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 218 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to inte

rnal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 219 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor

authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 220 Guidance:

Each control

must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 221 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms s

hould be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 222 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials

for staff and change ma

nagement records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 223 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing componen

ts are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 224 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 225 Guidance:

Each control must be enforced through both technical and procedural means. For

example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 226 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

A

ssessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 227 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforce
ment.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 228 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disa
bled to prevent unauthorized data transfer.

Practice 229 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 230 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for u

ser authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 231 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and poli

cy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 232 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may

implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted

VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 233 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 234 Guida

nce:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 235 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Lo

gging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 236 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for s

taff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 237 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Publ

ic-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 238 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 239 Guidance:

Each control must be enforced through both technical and pro

cedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 240 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant

to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 241 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof
of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 242 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials.
Public-facing components are isolated in a demilitarized zone (DMZ).
USB ports are disabled to prevent unauthorized data transfer.

Practice 243 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 244 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized ident

ity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 245 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may

implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, scr

eenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 246 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization impl

ements restricted VPN access to internal systems using role-based credentials. Public-facing

components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 247 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 248 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 249 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 250 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Traini

ng materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 251 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based

credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 252 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 253 Guidance:

Each control must be enforced through both

technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 254 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all ac
tivities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 255 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be
required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 256 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilita

rized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 257 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 258 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a

centralized identity provider for user authentication, combined with multi-factor authentication.

Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 259 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ens

ure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 260 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An

organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 261 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials

for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized

data transfer.

Practice 262 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 263 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined
with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:
Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:
An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 264 Guidance:
Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:
Ensure that logs, screenshots, and policy documents are available fo
r auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 265 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal system

s using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 266 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 267 Guidance:

Each control must be enf

orced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 268 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be us

ed to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 269 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management re

cords may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 270 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isol

ated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 271 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor

authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 272 Guidance:

Each control must be enforced through both technical and procedural means. For example, y
ou may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 273 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment C

onsiderations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 274 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real

-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 275 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to pre vent unauthorized data transfer.

Practice 276 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may

implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 277 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authent

ication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to

prevent unauthorized data transfer.

Practice 278 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy document

s are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 279 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access

to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 280 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 281 Guidance:

Each c

ontrol must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 282 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mecha

nisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 283 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and ch

ange management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 284 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing c

omponents are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 285 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 286 Guidance:

Each control must be enforced through both technical and procedural mea

ns. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 287 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the cont

rol.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials

for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 288 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 289 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports a
re disabled to prevent unauthorized data transfer.

Practice 290 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to

prevent unauthorized data transfer.

Practice 291 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provide

r for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 292 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, a

nd policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 293 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements rest

ricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 294 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 29

5 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 296 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authenticat

ion. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 297 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor

authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training material
s for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 298 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credential
s. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 299 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 300 Guidance:

Each control must be enforced through both technical

and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 301 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities re
levant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 302 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may

implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as

proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 303 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone

(DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 304 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 305 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralize

d identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 306 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that lo

gs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 307 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organizati

on implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 308 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transf

er.

Practice 309 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 310 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-

factor authentication. Logging mechanisms should be used to track all activities relevant to the

control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 311 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors.

Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 312 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using rol
e-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 313 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 314 Guidance:

Each control must be enforced throu

gh both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 315 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may

implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track
all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 316 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may a
lso be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials.

Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 317 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a d

emilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 318 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 319 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may impl

ement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 320 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Consideratio

ns:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 321 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Exam

ple:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 322 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauth

orized data transfer.

Practice 323 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor

authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 324 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, co

mbined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 325 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are avail

able for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 326 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials

for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal

systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 327 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 328 Guidance:

Each control must

be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 329 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms shoul

d be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials.

Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 330 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change manage

ment records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 331 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components a

re isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 332 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 333 Guidance:

Each control must be enforced through both technical and procedural means. For exa

mple, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 334 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Asses

sment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 335 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement

.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 336 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may

implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 337 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 338 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user

authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 339 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy d

ocuments are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 340 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN

access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 341 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 342 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials.

Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 343 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Loggin

g mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 344 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff

and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 345 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-f

acing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 346 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 347 Guidance:

Each control must be enforced through both technical and procedu

ral means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 348 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to t

he control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 349 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may

implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of o

ngoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 350 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB

ports are disabled to prevent unauthorized data transfer.

Practice 351 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 352 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity

provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 353 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screens

hots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 354 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implemen

ts restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 355 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Prac

tice 356 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 357 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor auth

entication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 358 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training m

aterials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 359 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based cre
dentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 360 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 361 Guidance:

Each control must be enforced through both tec

hnical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 362 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor

authentication. Logging mechanisms should be used to track all activi

ties relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 363 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be requ

ired as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to

prevent unauthorized data transfer.

Practice 364 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarize

d zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 365 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials

for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 366 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a cen

tralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 367 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure

that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 368 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An org

anization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 369 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data

transfer.

Practice 370 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 371 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 372 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for au

ditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 373 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems us

ing role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 374 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 375 Guidance:

Each control must be enforce

d through both technical and procedural means. For example, you may implement a centralized

identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 376 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used t

o track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to

prevent unauthorized data transfer.

Practice 377 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management record

s may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 378 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated

in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 379 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 380 Guidance:

Each control must be enforced through both technical and procedural means. For example, you m ay implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 381 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Consi

derations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials.

Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 382 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-wor

ld Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 383 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent

unauthorized data transfer.

Practice 384 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 385 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authenticat

ion, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 386 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents ar

e available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 387 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to i

nternal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 388 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor

authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 389 Guidance:

Each contr

ol must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 390 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanism

s should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 391 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials

for staff and change

management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 392 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing compo

nents are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 393 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 394 Guidance:

Each control must be enforced through both technical and procedural means.

For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 395 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 396 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enfo

rcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 397 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are d

isabled to prevent unauthorized data transfer.

Practice 398 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 399 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider fo

r user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 400 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and p

olicy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 401 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may

implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restrict

ed VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 402 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to

prevent unauthorized data transfer.

Practice 403 Gu

idance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 404 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication.

Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 405 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials fo r staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 406 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. P

ublic-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 407 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 408 Guidance:

Each control must be enforced through both technical and

procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 409 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities releva

nt to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 410 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as pro

of of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 411 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ
). USB ports are disabled to prevent unauthorized data transfer.

Practice 412 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 413 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized id

entity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 414 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may

implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs,

screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 415 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization i

mplements restricted VPN access to internal systems using role-based credentials. Public-facing

components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 416 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 417 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 418 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-fact
or authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 419 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Tra

ining materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 420 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-ba

sed credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 421 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 422 Guidance:

Each control must be enforced through b

oth technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 423 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all
activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 424 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also
be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 425 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demil

itarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 426 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 427 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implemen

t a centralized identity provider for user authentication, combined with multi-factor authentication.

Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 428 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 429 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 430 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthoriz

ed data transfer.

Practice 431 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 432 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may

implement a centralized identity provider for user authentication, combin

ed with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 433 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available

for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials.

Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 434 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal sys

tems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 435 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 436 Guidance:

Each control must be

enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 437 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 438 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 439 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are i

solated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 440 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 441 Guidance:

Each control must be enforced through both technical and procedural means. For example

, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 442 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessmen

t Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 443 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

R

eal-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 444 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 445 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may

implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 446 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user auth

entication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to

prevent unauthorized data transfer.

Practice 447 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy docum

ents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 448 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN acce

ss to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 449 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 450 Guidance:

Eac

h control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 451 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging me

chanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 452 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and

change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 453 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facin

g components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 454 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 455 Guidance:

Each control must be enforced through both technical and procedural

means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 456 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the c

ontrol.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials

for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 457 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoi

ng enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 458 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB port
s are disabled to prevent unauthorized data transfer.

Practice 459 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to

prevent unauthorized data transfer.

Practice 460 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity prov

ider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 461 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots

, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 462 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements r

estricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 463 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice

464 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 465 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authenti cation. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 466 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training mater ials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 467 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credent ials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 468 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 469 Guidance:

Each control must be enforced through both technic

al and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 470 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities
relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 471 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may

implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required

as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 472 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zo

ne (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 473 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 474 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a central

ized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 475 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that

logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 476 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organiz

ation implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 477 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data tra

nsfer.

Practice 478 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 479 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with mul

ti-factor authentication. Logging mechanisms should be used to track all activities relevant to the

control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 480 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for audito

rs. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 481 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using
role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 482 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 483 Guidance:

Each control must be enforced th

rough both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 484 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may

implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to tr
ack all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 485 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records ma
y also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials.

Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 486 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in

a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 487 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 488 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may i

mplement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 489 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considera

tions:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 490 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world E

xample:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 491 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent una

uthorized data transfer.

Practice 492 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor

authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 493 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication,

combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 494 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are av

ailable for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 495 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials

for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to inter

nal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 496 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 497 Guidance:

Each control m

ust be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 498 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms sh

ould be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials.

Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 499 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change man

agement records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 500 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing component

s are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 501 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 502 Guidance:

Each control must be enforced through both technical and procedural means. For

example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 503 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

As

sessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 504 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcem
ent.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 505 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may

implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disab
led to prevent unauthorized data transfer.

Practice 506 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 507 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for us

er authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 508 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and polic

y documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 509 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted V

PN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 510 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 511 Guidan

ce:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials.

Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 512 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Log

ging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 513 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for st

aff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 514 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Publi

c-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 515 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 516 Guidance:

Each control must be enforced through both technical and proc

edural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 517 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant t

o the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 518 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may

implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof o

f ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 519 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). U

SB ports are disabled to prevent unauthorized data transfer.

Practice 520 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 521 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identi

ty provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 522 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, scre

enshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 523 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization imple

ments restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 524 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

P

ractice 525 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 526 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor a uthentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 527 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Trainin
g materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 528 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 529 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 530 Guidance:

Each control must be enforced through both

technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 531 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor

authentication. Logging mechanisms should be used to track all act

ivities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 532 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be r

equired as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to

prevent unauthorized data transfer.

Practice 533 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitar

ized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 534 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials

for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 535 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a

centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 536 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensu

re that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 537 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An

organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 538 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized d

ata transfer.

Practice 539 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 540 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined w

ith multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 541 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 542 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems

using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 543 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 544 Guidance:

Each control must be enfo

rced through both technical and procedural means. For example, you may implement a centralized

identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 545 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be use
d to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to

prevent unauthorized data transfer.

Practice 546 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management rec

ords may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 547 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isola

ted in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 548 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 549 Guidance:

Each control must be enforced through both technical and procedural means. For example, yo
u may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 550 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Co

nsiderations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials.

Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 551 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-

world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 552 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prev ent unauthorized data transfer.

Practice 553 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 554 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authenti

cation, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 555 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents

are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 556 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access t

o internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 557 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 558 Guidance:

Each co

ntrol must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 559 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechan

isms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 560 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and cha

nge management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 561 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing co

mponents are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 562 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 563 Guidance:

Each control must be enforced through both technical and procedural mean

s. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials.

Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 564 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the contr
ol.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 565 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing e

nforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 566 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports ar

e disabled to prevent unauthorized data transfer.

Practice 567 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 568 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider

for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 569 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, an

d policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 570 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor

authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restr

icted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 571 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 572

Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 573 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authenticati

on. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 574 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 575 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials . Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 576 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to

prevent unauthorized data transfer.

Practice 577 Guidance:

Each control must be enforced through both technical a

nd procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 578 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities rel

evant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 579 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as
proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 580 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (
DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 581 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 582 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized

identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 583 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that log

s, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 584 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organizatio

n implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 585 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfe

r.

Practice 586 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials

for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 587 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-f
actor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 588 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors.

Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 589 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role

-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 590 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 591 Guidance:

Each control must be enforced throug

h both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 592 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track
all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 593 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may al

so be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 594 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a de

militarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 595 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 596 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may imple

ment a centralized identity provider for user authentication, combined with multi-factor

authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 597 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Consideration

s:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 598 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Examp

le:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 599 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials

for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unautho

rized data transfer.

Practice 600 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 601 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, com

bined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 602 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are availa

ble for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 603 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal

systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 604 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 605 Guidance:

Each control must

be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 606 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should

be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 607 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change managem

ent records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 608 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components ar

e isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 609 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may

implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 610 Guidance:

Each control must be enforced through both technical and procedural means. For exam

ple, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to

prevent unauthorized data transfer.

Practice 611 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assess

ment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 612 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 613 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 614 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 615 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user a

uthentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 616 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy do

cuments are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 617 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN a

ccess to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 618 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 619 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 620 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging

mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 621 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff

and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 622 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor

authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-fa

cing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 623 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 624 Guidance:

Each control must be enforced through both technical and procedur

al means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 625 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to th

e control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 626 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of on

going enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 627 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB p

orts are disabled to prevent unauthorized data transfer.

Practice 628 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials.

Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 629 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity p

rovider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 630 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screensh

ots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 631 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implement

s restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 632 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Pract

ice 633 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 634 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authe ntication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 635 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor

authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training ma

terials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 636 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based cred

entials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 637 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 638 Guidance:

Each control must be enforced through both tech

nical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials

for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 639 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activit

ies relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 640 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be requi

red as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 641 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials.

Public-facing components are isolated in a demilitarized

zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 642 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 643 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a cent

ralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 644 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure t

hat logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 645 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An orga

nization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 646 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data

transfer.

Practice 647 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 648 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with

multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 649 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for aud

itors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to

prevent unauthorized data transfer.

Practice 650 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems usi

ng role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 651 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials

for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 652 Guidance:

Each control must be enforced

through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 653 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to
track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 654 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records
may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 655 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated
in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 656 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 657 Guidance:

Each control must be enforced through both technical and procedural means. For example, you ma y implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 658 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Consid

erations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 659 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-worl

d Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 660 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent

unauthorized data transfer.

Practice 661 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor

authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 662 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authenticati

on, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 663 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are

available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 664 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials

for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to in

ternal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 665 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 666 Guidance:

Each contro

l must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 667 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms

should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials.

Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 668 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change

management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 669 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing compon

ents are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 670 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 671 Guidance:

Each control must be enforced through both technical and procedural means. F

or example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 672 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 673 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enfor
cement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 674 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor

authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are di
sabled to prevent unauthorized data transfer.

Practice 675 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 676 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for

user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 677 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and po

licy documents are available for auditors. Training materials for staff and change management

records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 678 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricte

d VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 679 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 680 Gui

dance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials.

Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 681 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication.

Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 682 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for

staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 683 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Pu

blic-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 684 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 685 Guidance:

Each control must be enforced through both technical and p

rocedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 686 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevan
t to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 687 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may

implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proo

f of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 688 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ)

. USB ports are disabled to prevent unauthorized data transfer.

Practice 689 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 690 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized ide

ntity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 691 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, s

creenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 692 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization im

plements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 693 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 694 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 695 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-facto
r authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 696 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Trai
ning materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 697 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-bas
ed credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 698 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 699 Guidance:

Each control must be enforced through bo

th technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.

Practice 700 Guidance:

Each control must be enforced through both technical and procedural means. For example, you may implement a centralized identity provider for user authentication, combined with multi-factor authentication. Logging mechanisms should be used to track all

activities relevant to the control.

Assessment Considerations:

Ensure that logs, screenshots, and policy documents are available for auditors. Training materials for staff and change management records may also be required as proof of ongoing enforcement.

Real-world Example:

An organization implements restricted VPN access to internal systems using role-based credentials. Public-facing components are isolated in a demilitarized zone (DMZ). USB ports are disabled to prevent unauthorized data transfer.