AD scan

AD CONTROL COVERAGE REPORT

What we *tested*, and *how*.

Absence of a finding is only assurance if the control was actually checked. This report lists the 26 checks run against north.sevenkingdoms.local, states what each one checked, and marks which came back clear.

CHECKS RUN	VERIFIED CLEAR	NEEDS ATTENTION
26	3	23

Generated November 16, 2026
Scope north.sevenkingdoms.local

COVERAGE SUMMARY TESTED IN THIS ENGAGEMENT

Every control here was *actively checked*.

Every control below was actively exercised during this assessment, and each entry states the check that was run: the attribute read, the protocol negotiated, the call issued. A control marked **verified clear** means that check was run and the weakness was not there, which is assurance you can put in front of a board or an auditor.

> Of the 26 checks run, 3 came back clear and 23 held a weakness. The clear ones are assurance you can cite, bounded to the scope listed; the rest are carried in full in your Security Assessment Report.

> Anexo II of the ENS holds 73 security measures. No system category is declared for this assessment, so it covers the 52 measures Anexo II requires at every category, and this report measures 12 of them. It also assesses one further measure whose exigibility follows the categorisation, so 13 measures in all. The remaining 40 are organisational, physical or personnel measures that cannot be observed from Active Directory, so they are neither assessed here nor reported as satisfied. Declaring the scope resolves the other 21 measures and moves the exigible total up or down from 52.

CHECKS RUN
26
one per distinct control area exercised across scope.

VERIFIED CLEAR
3
checked this engagement; no weakness present.

NEEDS ATTENTION
23
tested and present: tracked in the Security Assessment Report.

VERIFIED CLEAR 3 CHECKS

Checked. *Clean.*

Anonymous LDAP directory enumeration

VERIFIED CLEAR

2026-11-15

Checked: Performed an unauthenticated (anonymous) LDAP bind to the domain controller and attempted to read enabled user objects straight from the directory.

ASSURANCE · The directory rejected anonymous binds: no user, group, or policy object was readable without valid credentials, closing a common no-credential reconnaissance path against the domain.

ISO 27001:2022 A.5.15, A.8.20 **DORA** Art. 8 **ENS** op.acc.2 **NIS2** Art. 21(2)(e)
PCI DSS 4.0 Req. 7, Req. 8, Req. 11
CIS Windows Server 2.3.10.10, 2.3.10.2, 2.3.10.11, 2.3.10.1

Autologon credentials in Group Policy

VERIFIED CLEAR

2026-11-15

Checked: Inspected the Group Policy and registry autologon settings for a DefaultPassword stored in cleartext for automatic interactive logon.

ASSURANCE · No autologon credentials were present in Group Policy or the registry: no host is configured to log on automatically with a stored cleartext password.

ISO 27001:2022 A.5.17, A.8.9 **DORA** Art. 9(4)(d) **ENS** op.acc.5, mp.com.2
NIS2 Art. 21(2)(i), Art. 21(2)(h) **PCI DSS 4.0** Req. 2, Req. 8
CIS Windows Server 18.6.14.1

GPP cpasswords in SYSVOL

VERIFIED CLEAR

2026-11-15

Checked: Scanned every Group Policy Preferences XML file published in the SYSVOL share for the reversibly-encrypted cpassword attribute (the MS14-025 credential-leak class).

ASSURANCE · No Group Policy Preferences file in SYSVOL contained a cpassword attribute: the well-known domain-wide credential leak is confirmed absent, so no reader of SYSVOL can recover a stored password.

ISO 27001:2022 A.5.17, A.8.9 **DORA** Art. 9(4)(d) **ENS** op.acc.5, mp.com.2
NIS2 Art. 21(2)(i), Art. 21(2)(h) **PCI DSS 4.0** Req. 2, Req. 7, Req. 8
CIS Windows Server 18.6.14.1

TESTED & PRESENT 23 CHECKS

Tested, and *found* something.

These control areas were checked and a weakness was present. The full finding, severity, and step-by-step remediation live in your Security Assessment Report and AD Hardening Playbook.

Account Passwords Recovered in This Assessment

NEEDS ATTENTION

2026-11-15

Checked: Actively tested for this weakness against the assessed scope during the engagement.

PRESENT · Tested and found present. The finding, its severity and the step-by-step remediation are in your Security Assessment Report.

SECURITY ASSESSMENT REPORT → Account Passwords Recovered in This Assessment

ISO 27001:2022 A.5.17, A.8.5 **DORA** Art. 9(4)(d) **ENS** op.acc.5, op.acc.6
NIS2 Art. 21(2)(i), Art. 21(2)(j) **PCI DSS 4.0** Req. 8
CIS Windows Server 1.1.4, 1.1.5, 1.2.2

Accounts with Non-Expiring Passwords

NEEDS ATTENTION

2026-11-15

Checked: Read the userAccountControl flags of every enabled account for the bit that exempts it from password expiry, and separated the administrative accounts from the rest so the exposure is weighed by what each account can reach.

PRESENT · Enabled accounts are exempt from password expiry, so their credentials stay valid indefinitely, including any copy taken during an incident nobody detected.

SECURITY ASSESSMENT REPORT → Accounts with Non-Expiring Passwords

ISO 27001:2022 A.5.17 **DORA** Art. 6, Art. 9(4)(d) **ENS** op.acc.5
NIS2 Art. 21(2)(j), Art. 21(2)(i) **PCI DSS 4.0** Req. 8, Req. 12 **CIS Windows Server** 1.1.2

Anonymous account enumeration (null session / SAMR)

NEEDS ATTENTION

2026-11-15

Checked: Attempted an unauthenticated SMB null session against the domain controller and, through it, queried the SAM account database over MS-SAMR to list domain user accounts without any credentials.

PRESENT · An anonymous null session succeeded and enumerated 12 domain accounts over MS-SAMR, handing any unauthenticated network peer a complete target list for password spraying and account-based reconnaissance.

SECURITY ASSESSMENT REPORT → SMB Null Session Authentication on DC

ISO 27001:2022 A.8.20, A.8.5 **DORA** Art. 8 **ENS** op.acc.2, mp.com.3 **NIS2** Art. 21(2)(e)
PCI DSS 4.0 Req. 1, Req. 7, Req. 8, Req. 11
CIS Windows Server 2.3.10.10, 2.3.10.2, 2.3.10.12, 2.3.10.11, 2.3.10.1

Some accounts let the domain hand out password material with no login

NEEDS ATTENTION

2026-11-16

AS-REP Roasting

Checked: Read the userAccountControl flags of every enabled account for the one that waives Kerberos pre-authentication, then asked the domain controller for each such account's initial ticket without presenting any credential, to confirm the reply really is issued and really is encrypted with that account's password key.

PRESENT · The domain controller issued pre-authentication-free replies containing password-derived material, which anyone able to reach the domain controller can collect without holding an account.

SECURITY ASSESSMENT REPORT → AS-REP Roasting

ISO 27001:2022 A.5.17, A.8.5 **DORA** Art. 6, Art. 9(4)(d) **ENS** op.acc.5 **NIS2** Art. 21(2)(h), Art. 21(2)(j) **PCI DSS 4.0** Req. 8, Req. 11 **CIS Windows Server** 2.3.11.4, 1.1.4

Child Domain Can Escalate to Forest Root (Intra-Forest Trust)

NEEDS ATTENTION

2026-11-16

Checked: Actively tested for this weakness against the assessed scope during the engagement.

PRESENT · Tested and found present. The finding, its severity and the step-by-step remediation are in your Security Assessment Report.

SECURITY ASSESSMENT REPORT → Child Domain Can Escalate to Forest Root (Intra-Forest Trust)

ISO 27001:2022 A.5.18, A.8.2, A.8.22 **DORA** Art. 9(2), Art. 9(4)(c) **ENS** op.acc.4, org.4 **NIS2** Art. 21(2)(i) **PCI DSS 4.0** Req. 1, Req. 7, Req. 8, Req. 11 **CIS Windows Server** 2.2.28, 2.2.48

Some accounts can impersonate users to sensitive services

NEEDS ATTENTION

2026-11-16

Constrained Kerberos Delegation Misconfiguration

Checked: Read the msDS-AllowedToDelegateTo attribute and the TRUSTED_TO_AUTH_FOR_DELEGATION bit in userAccountControl on every account, identifying accounts configured to impersonate users to a named set of services and whether protocol transition is enabled (which lets the account obtain a ticket to those services without the user being involved).

PRESENT · An account can impersonate other users to the services listed in its msDS-AllowedToDelegateTo attribute, and where protocol transition is enabled it can do so unilaterally. The account and its allowed targets are named in your Security Assessment Report.

SECURITY ASSESSMENT REPORT → Constrained Kerberos Delegation Misconfiguration

ISO 27001:2022 A.5.18 **DORA** Art. 9(2) **ENS** op.acc.4 **NIS2** Art. 21(2)(i) **PCI DSS 4.0** Req. 7, Req. 8 **CIS Windows Server** 2.2.28

Credentials in account descriptions

NEEDS ATTENTION

2026-11-15

Checked: Scanned the description and comment attributes of every enumerable account for embedded passwords, keys, and other sensitive keywords.

PRESENT · 1 account description contained credential or sensitive material readable during enumeration: an immediately usable credential-disclosure path for any account that can read the directory.

SECURITY ASSESSMENT REPORT → **Credentials Stored in Directory Account Attributes**

ISO 27001:2022 A.5.17, A.8.3, A.8.5 **DORA** Art. 9(2), Art. 9(4)(d) **ENS** op.acc.5, mp.com.2 **NIS2** Art. 21(2)(i), Art. 21(2)(h) **PCI DSS 4.0** Req. 3, Req. 7, Req. 8

The domain controller still accepts NTLM logons at all

NEEDS ATTENTION

2026-11-15

Domain Controller Accepts NTLM Authentication

Checked: Attempted an NTLM authentication bind against the domain controller and read whether the bind was accepted rather than refused for a disabled authentication package. Acceptance is the protocol itself confirming NTLM is still a usable authentication path to the DC.

PRESENT · The domain controller accepts NTLM authentication. Captured or relayed NTLM material, and stolen password hashes, remain usable against it regardless of the NTLM version in use.

SECURITY ASSESSMENT REPORT → **Domain Controller Accepts NTLM Authentication**

ISO 27001:2022 A.8.5, A.8.20, A.8.9 **DORA** Art. 6, Art. 9(3), Art. 9(4)(d) **ENS** mp.com.2, mp.com.3, op.acc.2 **NIS2** Art. 21(2)(e), Art. 21(2)(h) **PCI DSS 4.0** Req. 2, Req. 8, Req. 11 **CIS Windows Server** 2.3.11.7, 2.3.11.10, 2.3.11.11, 2.3.8.1, 2.3.9.2, 2.3.9.5

The domain controller still accepts weak RC4 Kerberos encryption

NEEDS ATTENTION

2026-11-15

Domain Controller Accepts RC4 Kerberos Encryption

Checked: Sent a Kerberos pre-authentication request that offered only the RC4-HMAC encryption type (arcfour-hmac, etype 23) and read whether the domain controller issued a ticket under it rather than rejecting the request as an unsupported encryption type.

PRESENT · The domain controller issues Kerberos tickets under RC4-HMAC. A captured service ticket can be requested in the weaker cipher, which materially speeds up offline cracking such as Kerberoasting.

SECURITY ASSESSMENT REPORT → **Domain Controller Accepts RC4 Kerberos Encryption**

ISO 27001:2022 A.8.5, A.8.24, A.8.20 **DORA** Art. 6, Art. 9(3) **ENS** mp.com.2, op.acc.2 **NIS2** Art. 21(2)(e), Art. 21(2)(h) **PCI DSS 4.0** Req. 2, Req. 4, Req. 8, Req. 11 **CIS Windows Server** 2.3.11.4

The domain does not require strong AES Kerberos encryption

NEEDS ATTENTION

2026-11-15

Domain Does Not Force AES Encryption for Kerberos

Checked: Read the domain's Kerberos encryption policy and confirmed whether AES is merely supported or actually enforced: a request that offers RC4 alongside AES was made, and the domain controller's willingness to serve the RC4 ticket shows RC4 is still a negotiable fallback.

PRESENT · The domain does not force AES. RC4 stays a negotiable fallback, so any client that asks for an RC4 ticket is given one, reopening the weak-cipher exposure even where AES is available.

SECURITY ASSESSMENT REPORT → **Domain Does Not Force AES Encryption for Kerberos**

ISO 27001:2022 A.8.5, A.8.24, A.8.20 **DORA** Art. 6, Art. 9(3) **ENS** mp.com.2, op.acc.2 **NIS2** Art. 21(2)(e), Art. 21(2)(h) **PCI DSS 4.0** Req. 2, Req. 8, Req. 11 **CIS Windows Server** 2.3.11.4

Service-account passwords can be pulled from the domain and cracked offline

NEEDS ATTENTION

2026-11-16

Kerberoasting

Checked: Enumerated every account carrying a servicePrincipalName and requested a service ticket for it, then examined the encryption type the domain controller issued: a ticket encrypted with the account's own password key is material any authenticated user can take away and attack offline.

PRESENT · Service tickets were obtainable for accounts whose password key encrypts them, giving any authenticated user material to attack offline at their own pace and without further contact with the domain.

SECURITY ASSESSMENT REPORT → **Kerberoasting**

ISO 27001:2022 A.8.2, A.5.17, A.8.5 **DORA** Art. 6, Art. 9(4)(d) **ENS** op.acc.5, op.acc.4 **NIS2** Art. 21(2)(h), Art. 21(2)(j) **PCI DSS 4.0** Req. 8, Req. 11 **CIS Windows Server** 2.3.11.4, 1.1.4

Web-service logons can be coerced and relayed onward

NEEDS ATTENTION

2026-11-15

Kerberos Web Service (HTTP SPN) Relay and Coercion Surface

Checked: Enumerated the servicePrincipalName attribute across the directory for HTTP-class service principal names and identified the web-facing services whose authentication can be coerced and relayed onward, because a coerced HTTP authentication becomes a relay surface wherever the receiving service does not enforce channel binding or signing.

PRESENT · One or more services register an HTTP service principal name whose authentication can be coerced and relayed to another service. The services are named in your Security Assessment Report.

SECURITY ASSESSMENT REPORT → **Kerberos Web Service (HTTP SPN) Relay and Coercion Surface**

ISO 27001:2022 A.8.20, A.8.5, A.8.22 **DORA** Art. 9(4)(b) **ENS** mp.com.3, mp.com.2 **NIS2** Art. 21(2)(h), Art. 21(2)(e) **PCI DSS 4.0** Req. 1, Req. 2, Req. 4, Req. 8, Req. 11 **CIS Windows Server** 2.3.9.2, 2.3.8.1, 2.3.5.4, 2.3.5.3, 2.3.9.5

KRBTGT account key rotation

NEEDS ATTENTION

2026-11-15

Checked: Read the KRBTGT account's password age from the directory to establish whether the key that signs every Kerberos ticket in the domain has been rotated within policy.

PRESENT · The KRBTGT key is outside its rotation window, so a key recovered at any point in the past still signs valid tickets today.

SECURITY ASSESSMENT REPORT → krbtgt Account Password Not Rotated

ISO 27001:2022 A.8.5, A.8.2, A.8.17 **DORA** Art. 9(4)(d) **ENS** op.acc.5, mp.com.3, op.exp.10
NIS2 Art. 21(2)(h), Art. 21(2)(i) **PCI DSS 4.0** Req. 7, Req. 8, Req. 11
CIS Windows Server 2.2.48, 2.3.11.4

The directory does not enforce protected LDAP connections

LDAP Signing / Channel Binding Not Hardened

NEEDS ATTENTION

2026-11-15

Checked: Opened an LDAP connection to the domain controller and observed how it answers a simple bind that carries no integrity protection: whether the directory returns strongerAuthRequired to demand LDAP signing, and whether a TLS-wrapped bind is rejected for a missing channel-binding token. Those two responses are what say, from the wire, whether signing and channel binding are enforced.

PRESENT · The domain controller accepts an LDAP bind without signing or without a channel-binding token. Authentication captured or coerced from another host can be relayed straight to the directory and acted on in the victim's context.

SECURITY ASSESSMENT REPORT → LDAP Signing / Channel Binding Not Hardened

ISO 27001:2022 A.8.20, A.8.21, A.8.5 **DORA** Art. 6, Art. 9(2), Art. 9(3)
ENS mp.com.2, mp.com.3, op.acc.2 **NIS2** Art. 21(2)(e), Art. 21(2)(h)
PCI DSS 4.0 Req. 1, Req. 2, Req. 8, Req. 11 **CIS Windows Server** 2.3.5.4, 2.3.5.3, 2.3.11.9

Credential memory on hosts is left unprotected

LSASS Not Running as a Protected Process (RunAsPPL Disabled)

NEEDS ATTENTION

2026-11-15

Checked: Read the RunAsPPL value under HKLM\SYSTEM\CurrentControlSet\Control\Lsa on each assessed host and determined whether the LSA process is configured to run as a protected process, which stops an ordinary administrator from reading credential material out of its memory.

PRESENT · LSA protection is not enabled, so an administrator on the host can read the credentials cached in the LSA process's memory. The affected hosts are named in your Security Assessment Report.

SECURITY ASSESSMENT REPORT → LSASS Not Running as a Protected Process (RunAsPPL Disabled)

ISO 27001:2022 A.8.24, A.5.17 **DORA** Art. 9(4)(d), Art. 9(3) **ENS** op.exp.2, mp.com.2
NIS2 Art. 21(2)(h), Art. 21(2)(i) **PCI DSS 4.0** Req. 3, Req. 8, Req. 2
CIS Windows Server 18.9.26.2

Ordinary users can create their own computer accounts

NEEDS ATTENTION

2026-11-15

Machine Account Quota Allows Domain Join

Checked: Read ms-DS-MachineAccountQuota from the domain object to establish how many computer accounts an ordinary user may create. A computer account is a domain identity, so this value decides whether an ordinary user can mint one.

PRESENT · Ordinary users may create computer accounts, giving any authenticated user a domain identity of their own making: the starting point for several delegation and relay techniques.

SECURITY ASSESSMENT REPORT → Machine Account Quota Allows Domain Join

ISO 27001:2022 A.5.18, A.8.2 **DORA** Art. 9(2) **ENS** op.acc.4, org.4 **NIS2** Art. 21(2)(i) **PCI DSS 4.0** Req. 7, Req. 8 **CIS Windows Server** 2.2.28

The domain controller is vulnerable to a known privilege-escalation flaw

NEEDS ATTENTION

2026-11-16

noPac/sAMAccountName Spoofing (CVE-2021-42278 + CVE-2021-42287)

Checked: Asked the domain controller for a Kerberos ticket twice for the same account, once with the privilege attribute certificate requested and once without, and compared the two. A patched controller returns tickets of the same shape; the unpatched defect shows as a materially smaller ticket without the certificate.

PRESENT · The domain controller's ticket-granting behaviour matches the unpatched defect, which takes an ordinary domain user to full domain control.

SECURITY ASSESSMENT REPORT → noPac/sAMAccountName Spoofing (CVE-2021-42278 + CVE-2021-42287)

ISO 27001:2022 A.8.8, A.8.5 **DORA** Art. 9(2), Art. 9(4)(f) **ENS** op.acc.5, op.acc.3 **NIS2** Art. 21(2)(e), Art. 21(2)(i) **PCI DSS 4.0** Req. 6, Req. 8, Req. 11 **CIS Windows Server** 2.2.48, 2.3.6.5

Passwords Predating Current Policy

NEEDS ATTENTION

2026-11-15

Checked: Took the timestamp of the last change to each password policy from its per-attribute replication metadata (which records when the policy attributes themselves were modified, not when the object was last touched) and compared each enabled account's pwdLastSet against the policy that applies to it.

PRESENT · Enabled accounts still hold a password set before the governing policy was last changed. Active Directory does not apply a policy change retroactively, so those credentials were never required to meet the current rules.

SECURITY ASSESSMENT REPORT → Passwords Predating Current Policy

ISO 27001:2022 A.5.17, A.8.5 **DORA** Art. 6, Art. 9(4)(d) **ENS** op.acc.5, op.acc.4 **NIS2** Art. 21(2)(j), Art. 21(2)(i) **PCI DSS 4.0** Req. 8, Req. 12 **CIS Windows Server** 1.1.1, 1.1.2

Print services are vulnerable to a known remote code-execution flaw

NEEDS ATTENTION

2026-11-16

PrintNightmare (CVE-2021-34527) Exposure in the Print Spooler

Checked: Bound to the print spooler service on each reachable host and submitted a deliberately empty driver-installation request, reading the return code to distinguish a host that refuses the call outright from one that accepts it and only rejects the malformed contents.

PRESENT · Hosts accepted a remote driver-installation request. The spooler runs with the highest local privilege, so code loaded this way runs as the machine itself.

SECURITY ASSESSMENT REPORT → PrintNightmare (CVE-2021-34527) Exposure in the Print Spooler

ISO 27001:2022 A.8.8, A.8.9 **DORA** Art. 9(4)(f) **ENS** op.exp.4 **NIS2** Art. 21(2)(e)
PCI DSS 4.0 Req. 2, Req. 6, Req. 11 **CIS Windows Server** 18.7.1, 5.1

Privileged sessions on lower-tier hosts

NEEDS ATTENTION

2026-11-16

Checked: Enumerated the interactive and service sessions on reachable hosts and cross-referenced each logged-on principal's privilege tier against the tier of the host it was signed in to.

PRESENT · Higher-tier accounts were signed in to one or more lower-tier hosts, placing a privileged credential in the memory of a machine that a lower-tier compromise reaches.

SECURITY ASSESSMENT REPORT → Privileged Sessions on Lower-Tier Hosts

ISO 27001:2022 A.8.2, A.5.18, A.8.18 **DORA** Art. 9(4)(c) **ENS** op.acc.6, op.acc.3
NIS2 Art. 21(2)(i) **PCI DSS 4.0** Req. 7, Req. 8 **CIS Windows Server** 2.2.2

Sensitive data in reachable shares

NEEDS ATTENTION

2026-11-15

Checked: Walked the shares readable with the assessment credential and inspected their contents for stored passwords, keys, and configuration secrets.

PRESENT · Secret material was recoverable from readable shares, giving any account with the same reach a further credential to use.

SECURITY ASSESSMENT REPORT → Sensitive Data Found in SMB Shares

ISO 27001:2022 A.5.17, A.8.3 **DORA** Art. 9(4)(d) **ENS** mp.com.2, op.exp.2
NIS2 Art. 21(2)(i) **PCI DSS 4.0** Req. 3, Req. 7, Req. 8
CIS Windows Server 2.3.10.12, 2.3.10.5

SMB message signing (relay resistance)

NEEDS ATTENTION

2026-11-15

Checked: Read the SMB signing policy advertised by each reachable host to identify any that would accept a relayed authentication.

PRESENT · One or more hosts do not require SMB message signing and would accept an authentication relayed from elsewhere in the domain.

SECURITY ASSESSMENT REPORT → SMB Signing Not Required

ISO 27001:2022 A.8.20, A.8.21, A.8.22 **DORA** Art. 9(4)(b) **ENS** mp.com.3, mp.com.2
NIS2 Art. 21(2)(h), Art. 21(2)(e) **PCI DSS 4.0** Req. 1, Req. 2, Req. 4, Req. 8, Req. 11
CIS Windows Server 2.3.9.2, 2.3.8.1, 2.3.9.5, 18.6.8.2, 18.6.7.1

Weak Default Domain Password Policy

NEEDS ATTENTION

2026-11-15

Checked: Read the Default Domain Password Policy from the domain object and measured three values against the CIS benchmark and the Microsoft security baseline: the account lockout threshold, the minimum password length, and whether the complexity requirement is in force.

PRESENT · One or more of the lockout, length and complexity settings sit below the published baseline, lowering the cost of guessing attacks against every account the policy governs.

SECURITY ASSESSMENT REPORT → Weak Default Domain Password Policy

ISO 27001:2022 A.5.17, A.8.5 **DORA** Art. 6, Art. 9(4)(d) **ENS** op.acc.5

NIS2 Art. 21(2)(j), Art. 21(2)(i) **PCI DSS 4.0** Req. 8, Req. 12

CIS Windows Server 1.1.4, 1.1.5, 1.2.2

SCOPE OF THIS ATTESTATION

This report attests to the checks ADscan actively ran in this engagement, one per control area listed. A control area that does not appear above was not assessed, which is not the same as clear: only the entries listed were exercised, and only those marked verified clear carry positive assurance. Coverage is bounded by the scope, the credentials, and the network reachability of this assessment.