Amethyst Cyber Group
Common Sense Cyber Security

CLIENT CONFIDENTIAL

PREREQUISITES CHECKLIST

Managed Vulnerability Scanning Prerequisites

Information and access required before a managed scanning programme begins.

CLIENT	DOCUMENT REF
[Client Organisation]	ACG-PRE-MVS
VERSION	**ISSUED**
2.0	June 2026

Purpose. Complete this checklist before the scanning programme begins. Return completed items to your Amethyst Cyber Group project contact. Do not send credentials by email — use the agreed secure channel.

Managed Vulnerability Scanning Prerequisites

Complete all sections relevant to your scanning scope. Tick each item when the information has been provided or confirmed.

Asset Inventory and Scope Definition

- [ ] Provide a complete asset list: all domains, hostnames, external IP addresses, and CIDR ranges to be scanned.
- [ ] Confirm cloud assets in scope: AWS account IDs, Azure subscription IDs, Google Cloud project IDs, or Oracle Cloud tenancy details.
- [ ] Provide a list of explicitly excluded assets — systems that must not be scanned under any circumstances.
- [ ] Identify fragile or legacy systems (OT, industrial controllers, older operating systems) that require reduced scan intensity or manual exclusion.
- [ ] Confirm whether subdomain or host discovery is authorised beyond the provided asset list, and the extent of enumeration permitted.
- [ ] Confirm ownership of all in-scope IP addresses and domains — third-party hosted services must be confirmed as within the client's authorisation to scan.

Scan Cadence and Scheduling

- [ ] Confirm the scan cadence: weekly, monthly, quarterly, or continuous (always-on) scanning.
- [ ] Confirm maintenance windows and time-of-day restrictions — specify periods during which scanning must not occur.
- [ ] Confirm change freeze periods (e.g., month-end, major release windows) when scanning should be paused.
- [ ] Confirm rate limiting requirements for fragile or bandwidth-constrained environments.
- [ ] Confirm reporting cadence: when scan reports are expected and who receives them.
- [ ] Confirm whether ad-hoc emergency scans are permitted outside the agreed schedule, and who can request them.

Authenticated Scanning

- [ ] Confirm whether authenticated scanning is required for web applications, internal hosts, or both.
- [ ] For web application authenticated scanning: provide a dedicated scanner account for each application role, with username, password, and MFA bypass or dedicated TOTP seed.
- [ ] For host-based authenticated scanning: provide a local or domain account with sufficient privileges for the scanning tool (administrator for Windows, sudo-enabled for Linux).
- [ ] For cloud authenticated scanning: provide a service principal, IAM user, or read-only scanning role with appropriate permissions.
- [ ] Confirm the process for credential rotation — scanning credentials must remain valid for the programme duration or be rotated with advance notice.

- [ ] Confirm whether a dedicated scanner agent will be deployed on internal hosts, and provide approval for agent installation.
- [ ] Do not send credentials by email. Provide credentials via password manager share, secure file transfer, or the agreed encrypted channel.

Network Access and Allow-Listing

- [ ] Provide firewall rule changes or allow-list entries to permit scanner source IP addresses to reach all in-scope targets.
- [ ] Confirm VPN or network access method for internal scanning: agent-based, appliance placement, or VPN tunnel to scanner infrastructure.
- [ ] Confirm WAF and IDPS exemptions for scanner source IPs to prevent false blocking of scan traffic.
- [ ] Confirm SOC or monitoring team notification route — provide the team contact who should be informed when scanning begins to avoid false-positive incidents.
- [ ] For cloud scanning, confirm whether scanner access is via the public internet, a private link, or a dedicated scanning role with network access.

External Scanning

- [ ] Confirm whether external unauthenticated scanning covers the full internet-facing estate or a defined subset.
- [ ] Confirm CDN or DDoS mitigation is aware of scanner IPs to avoid rate-limiting or blocking scan traffic.
- [ ] Confirm whether the external scan should include TLS / certificate analysis, open port enumeration, and service version detection.

Internal Scanning

- [ ] Confirm internal network segments in scope: corporate LAN, server VLANs, DMZ, cloud-connected segments, remote access segments.
- [ ] Confirm whether Windows, Linux, macOS, and network device scanning are all in scope.
- [ ] Confirm Active Directory integration requirements if applicable — domain name and domain controller addresses.
- [ ] Confirm whether network device scanning (switches, routers, firewalls) is in scope and provide SNMP community strings or SSH credentials if required.

Vulnerability Management and Remediation Process

- [ ] Provide named vulnerability management owners: the individual responsible for reviewing findings and driving remediation.
- [ ] Confirm remediation SLAs by severity: expected timeframes for addressing Critical, High, Medium, and Low findings.
- [ ] Confirm the ticketing or workflow integration: Jira, ServiceNow, Azure DevOps, or manual process for tracking remediation.
- [ ] Confirm the exception and risk acceptance process: who can authorise a vulnerability exception, and for how long.
- [ ] Confirm escalation contacts for critical findings discovered between scheduled reports — provide a direct contact for out-of-hours notification of critical vulnerabilities.

- [ ] Confirm whether remediation validation scans are included in scope or require separate scheduling.