Amethyst Cyber Group
Common Sense Cyber Security

CLIENT CONFIDENTIAL

PREREQUISITES CHECKLIST

Governance and Compliance Prerequisites

Information required before Cyber Essentials, CIS, build review, or control evidence work begins.

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

Purpose. Complete the sections relevant to your governance driver. Not all sections will apply — focus on the areas matching your compliance requirement or assessment type.

Governance and Compliance Prerequisites

Complete all sections relevant to your engagement type. Items marked for specific assessments (Cyber Essentials, CIS, build review) only need to be completed if that assessment type is in scope.

General — All Engagements

- [ ] Confirm the governance driver: Cyber Essentials certification, optional readiness assessment, CIS Benchmark alignment, build review, supplier assurance, internal audit, or another compliance requirement.
- [ ] Provide a named project contact and a technical contact who has access to configuration evidence, management consoles, and relevant IT systems.
- [ ] Define the scope boundary: business units, locations, cloud tenants, endpoints, servers, SaaS platforms, network devices, and any explicit exclusions.
- [ ] Confirm the desired timeline and any external deadlines (e.g., certification submission date, customer audit date, board review date).
- [ ] Do not send credentials, private keys, or sensitive access material by email — use the agreed secure channel.

Cyber Essentials Certification

- [ ] Confirm whether this is a Cyber Essentials (self-assessment) or Cyber Essentials Plus (independently verified) submission.
- [ ] Define the certification scope: all devices and cloud services under the organisation's control, or a defined subset with clear boundaries.
- [ ] Prepare evidence for the five control areas: boundary firewalls and internet gateways, secure configuration, user access control, malware protection, and patch management / security update management.
- [ ] For firewalls: provide firewall rule sets or management console access for each boundary device, including cloud security groups and virtual firewalls.
- [ ] For secure configuration: confirm how default accounts are handled, unnecessary services are disabled, and auto-run is controlled across endpoints, servers, and network devices.
- [ ] For user access control: confirm the process for account provisioning and removal, privileged account management, and MFA enforcement for internet-accessible services.
- [ ] For malware protection: confirm AV or EDR product, version, update frequency, and coverage across the in-scope estate.
- [ ] For patch management: confirm patch policy, patch cadence, and how unsupported software is identified and managed within the scope.
- [ ] Confirm the desired submission timeline and whether any known gaps require remediation before submission.

Cyber Essentials Readiness

- [ ] Confirm the review depth: gap analysis only, or full evidence review with remediation recommendations.

- [ ] Identify known gaps or areas of concern before the review begins — this speeds up the readiness assessment.
- [ ] Provide access to device management platforms where relevant: Microsoft Intune, Microsoft Endpoint Configuration Manager (MECM), Jamf, or equivalent.
- [ ] Provide access to cloud management consoles for AWS, Azure, Google Cloud, or SaaS platforms in scope.
- [ ] Confirm remediation owners for each control area — who is responsible for fixing identified gaps before submission.

CIS Benchmark Alignment

- [ ] Confirm benchmark versions and target profiles (Level 1 or Level 2) for each platform type in scope: Windows endpoints, Windows Server, macOS, Linux, network devices, cloud foundations.
- [ ] Confirm cloud-specific benchmarks in scope: CIS Azure Foundations, CIS AWS Foundations, CIS Google Cloud Foundations, CIS Microsoft 365 Foundations.
- [ ] Provide configuration exports or management console access: Group Policy Objects (GPOs), Intune compliance policies, Jamf profiles, Chef / Ansible configs, or equivalent.
- [ ] Provide cloud policy exports: Azure Policy assignments, AWS Config rules, GCP Organisation Policies, or equivalent IaC (Terraform, Bicep, CloudFormation).
- [ ] Confirm whether benchmark alignment is a target state or a starting point — and whether deviations from benchmark are expected due to operational constraints.
- [ ] Provide a list of known accepted deviations with documented business justification and risk owner sign-off.

Secure Build Review

- [ ] Confirm the platform types in scope: Windows, Linux, macOS, containerised workloads, network devices, or cloud service configurations.
- [ ] Provide access to a representative sample of in-scope systems: at minimum one example of each build type (e.g., standard workstation, server build, cloud VM image).
- [ ] Provide existing build documentation: hardening guides, baseline configs, standard operating environment (SOE) documents, or golden images.
- [ ] Confirm the review approach: automated tool-based scan of live systems, export-based review of config files, or manual walkthrough with system administrators.
- [ ] Confirm whether container images, Kubernetes configurations, or Helm charts are in scope, and provide access to image registries or Kubernetes cluster configs.
- [ ] Provide operational constraints that affect hardening decisions — services that cannot be disabled, legacy software that cannot be patched, or business processes that require specific configuration.

Evidence and Reporting

- [ ] Confirm the report audience and format: technical gap report, executive summary, certification evidence pack, or board-level risk paper.
- [ ] Confirm accepted deviations, compensating controls, and business owners for risk acceptance decisions — these should be documented before the review closes.
- [ ] Confirm remediation deadlines and whether a follow-up review is required to validate that identified gaps have been addressed.