Apptega

GUIDE

CIS Controls v8.1

Compliance Guide

Current as of October 2, 2025

Apptega

Purpose

Convert CIS Controls v8.1 (Controls 1–18) into a practical, auditable security program. This guide specifies owners, Implementation Group (IG1/IG2/IG3) targets, acceptance criteria, evidence, monitoring, internal audit, management review, and corrective actions. Each control follows a consistent pattern: Intent → Minimums (by IG) → Implement → Evidence → Acceptance Criteria → Common Failures → Internal QA → Docs: Program sections include organization-defined parameters (ODPs), applied narratives, operating calendars, templates, and an auditor-ready evidence pack.

How to use this guide

1. Establish a working baseline with the 90-Day Quick-Start.
2. Apply the Standards & Practices section control-by-control.
3. Set thresholds in ODPs; catalog artifacts in the Evidence Register.
4. Run the loop: Continuous Monitoring → Internal Audit → Management Review → Corrective Action → Change Management.
5. Use annexes for auditor handoffs, exception governance, provider matrices, and communications.

Apptega

1. Introduction 4
2. Scope & IG Targeting (Where IG1/IG2/IG3 apply) 7
3. Roles & Responsibilities (RACI) 8
4. CIS v8.1 at a Glance — Outcomes by Control 9
5. Standards & Practices (Deep Dives by Control, IG-mapped) 10
6. Organization-Defined Parameters (ODPs) & Metric Definitions 21
7. Evidence Register (Authoritative Artifacts) 23
8. Continuous Monitoring (KRIs, Alerts, Automation) 24
9. Internal Audit Program (CIS v8.1) 24
10. Management Review (Security Governance) 25
11. Corrective Action (RCA/CAPA) Workflow 26
12. Change Management for Security-Impacting Changes 26
13. Evidence Sampling Plans (Internal QA) 27
14. Common Pitfalls & Anti-Patterns 27
15. Cloud & Hosting Scenarios — CIS Shared-Responsibility Mapping 28
16. Evidence & Documentation Checklist 29
17. Training & Competence (Role Rubrics) 29
18. FAQs (Executives & Auditors) 30
19. Self-Assessment & Leadership Attestation 31
20. References 32
21. Minimal Policy Set 32
22. Communications Plan & Templates 33
Annex A — Control→Safeguard Mapping (IG1 / IG2 / G3 selection) 34
Annex B — Sample Auditor Evidence Pack (CIS v8.1) 34
Annex C — Templates 35

1. Introduction

The CIS Controls v8.1 define a prioritized, risk-based set of security practices that reduce the most common and consequential cyber threats. This guide turns those practices into a cohesive operating program your organization can adopt, measure, and defend during audits—without relying on any other framework. It explains what to implement, who owns it, how to prove it works, and how to keep it effective over time.

Apptega

What this guide delivers

- A program blueprint for CIS v8.1 across Implementation Groups (IG1–IG3), including clear ownership, thresholds, and
- Practical procedures for deploying and sustaining safeguards in enterprise settings (endpoints, servers, network, cloud, SaaS, identities, and service providers).
- A governance loop that links day-to-day operations to executive oversight: continuous monitoring, internal audit, management review, and corrective actions.
- Ready-to-use registers, templates, operating calendars, and role rubrics so teams can execute consistently and auditors can verify quickly.

Who should use it

Security leadership, GRC, SecOps, IAM, Platform/Cloud, Network Engineering, Application Security, Incident Response, Procurement/TPRM, and Internal Audit

How to work with it

Begin with the 90-Day Quick-Start to establish core hygiene, select IG targets per environment, and stand up monitoring. Use the Standards & Practices section to implement safeguards in a consistent way. Set measurable thresholds in the ODPs, file evidence to the register as you go, and run the governance cycle on the defined cadence. The annexes provide auditor-ready packs, exception governance, provider responsibility matrices, and communications templates.

What “good” looks like

- Coverage is known and trended (inventories, logging, EDR, backups).
- Time-bound SLAs are met (patching, detections, restores, remediation).
- Exceptions are rare, compensated, and time-boxed with explicit expiry.
- Findings drive improvements that are verified for effectiveness.
- Leadership sees clear status, risks, and decisions in each review.

Apptega

1A. 90-Day Quick-Start (IG1 foundation → IG2 ramp)

Days 1—15: Stand up core hygiene

- Adopt CIS v8.1; declare IG targets per environment.
- Enable automated asset discovery and software inventory (C1–C2).
- Publish secure configuration baselines (C4) and patch SLAs (C7).
- Enforce MFA for administrative and remote access (C6).
- Centralize audit logs (C8). Deploy EDR with tamper protection (C10).
- Approve Incident Response Plan and schedule a tabletop (C17).

Days 16—45: Implement critical safeguards

- Raise asset inventory coverage to ≥98%; quarantine unknowns automatically (C1).
- Enforce software allow-listing on servers and admin workstations (C2).
- Apply baselines via configuration management; enable drift alerting and remediation (C4).
- Harden email/web (gateway filtering, attachment sandboxing, DMARC enforcement) (C9).
- Configure backups with at least one restore test (C11)
- Define ODPs & KRIs (Section 6/8).

Days 46—90: Evidence & audit readiness

- Run an internal audit of MFA, EDR, patch SLAs, backups, logging (Section 9).
- Approve annual pen-test scope (C18).
- Hold Management Review: approve exceptions with expiry, close actions, fund gaps, lock IG2 rollout dates.

2. Scope & IG Targeting (Where IG1/IG2/IG3 apply)

- **Scope:** Enterprise-managed and BYOD endpoints, servers, network devices, virtual/cloud workloads, identities (human and service), applications (on-prem/SaaS), networks, data stores, and service providers with access to business data or operations.
- **IG application:** IG1 baseline for all environments; IG2 for internet-facing, revenue-critical, or sensitive-data zones; IG3 for crown-jewel systems and high-exposure segments.
- **Acceptance Criteria:** Documented scope with environment-level IG declarations; exceptions justified, compensating-controlled, and time-boxed with review dates.

2A. IG Targeting Method (Scoring Rubric)

Score each environment 1–5 in: Internet Exposure, Data Sensitivity, Business Criticality, Lateral Movement Risk, Regulatory Drivers.

- **IG1:** total ≤9
- **IG2:** total 10–15
- **IG3:** total ≥16

  Review semiannually or on material change (new exposure, data class, M&A). Keep an IG Assignment Table with scores, owners, and next review date.

3. Roles & Responsibilities (RACI)

Program Area	Accountable	Responsible	Consulted	Informed
CIS adoption & IG targets	CISO	GRC Lead	Legal, HR	IT/Sec Leads
Asset & software inventories	CIO	ITAM Lead	SecOps, App Owners	Finance
Secure config & patching	CISO	Platform Eng, SecOps	App Owners	IT
Identity & access	CISO	IAM Lead	HR, Audit	All
Logging & monitoring	CISO	SecOps	Platform Eng	App Owners
Email/web & malware	CISO	SecOps	IT	All
Backups & recovery	CIO	IT Ops	App Owners	SecOps
Network mgmt & defense	CISO	NetEng, SecOps	App Owners	IT
Training & awareness	HR	L&D, GRC	SecOps	All
Service providers	CFO	TPRM Lead	Security, Legal	Business Units
IR & pen-testing	CISO	IR Lead, Red Team	Legal, PR	Executives

3A. Program Operating Model (Decision Rights & Escalations)

Decision Rights

- IG assignment per environment: CISO (A); GRC (R); Infra/App owners (C).
- Exception approvals & expiry: CISO or delegate (A); Control Owner (R); GRC (C).
- Pen-test scope & schedule: CISO/IR (A); Red Team (R); App/Infra owners (C).
- Provider tiering & minimums: CISO (A); TPRM Lead (R); Legal/SecOps (C).
- Quarterly Operating Calendar: CISO (A); GRC (R); Control Owners (C).

Escalations

- SLA/KRI red for 2 consecutive periods → escalate to Management Review with corrective-action plan & date.
- Any exception past expiry → immediate block or alternate control within 48 hours; reported in next review.

4. CIS v8.1 at a Glance — Outcomes by Control

Control	Intended Outcome When "Good"
1 Asset Inventory	All assets continuously discovered and recorded; unmanaged assets blocked or enrolled fast.
2 Software Inventory	Only authorized software executes; unauthorized software removed quickly.
3 Data Protection	Sensitive data classified, encrypted, and governed; exfiltration risks managed.
4 Secure Configuration	Hardened baselines enforced; configuration drift detected and remediated.
5 Account Management	Accounts lifecycle-managed; stale, orphaned, and shared accounts eliminated.
6 Access Control Management	Least privilege and MFA enforced; privileged elevation time-bound and logged.
7 Vulnerability Management	Risk-based remediation within SLAs; exceptions controlled and expiring.
8 Audit Log Management	Centralized, protected, actionable logging with retention and alerting.
9 Email & Web Protections	Phishing/malware from email/web mitigated; domains protected.
10 Malware Defenses	Modern endpoint defenses with high coverage and timely detections.
11 Data Recovery	Resilient backups and proven restores for critical systems and data.
12 Network Infra Mgmt	Devices hardened; configs versioned; unauthorized changes prevented.
13 Network Monitoring & Defense	Effective visibility and detections across network paths and cloud.
14 Security Awareness & Skills	People trained; risky behaviors measured and reduced.
15 Service Provider Management	Providers meet security obligations; notices and telemetry handled.
16 Application Software Security	Secure SDLC with testing and signed, trustworthy releases.
17 Incident Response	Prepared, practiced, and measured incident handling.
18 Penetration Testing	Planned testing validates defenses and drives measurable fixes.

4A. Risk-Based Prioritization Playbook

Scoring Factors: Exploitability, External Exposure, Blast Radius, Detectability, Compensating Controls.

Process:

1. Score backlog items 1–5 per factor; compute total.
2. Tie-breakers: (a) external exposure wins; (b) items with weak detectability move up; (c) items with no compensating controls move up.
3. Publish top 10 items each month; track closure rate and age.

Output: A single prioritized remediation board feeding patching, baseline drift, EDR gaps, logging scope, provider actions.

Apptega

5. Standards & Practices (Deep Dives by Control, IG-mapped)

(Full, non-placeholder content for each control follows the approved pattern.)

5.1 Control 1 — Inventory and Control of Enterprise Assets

Intent: Maintain a complete, accurate inventory; prevent or rapidly remediate unmanaged assets.

Minimums: (IG1/IG2/IG3). IG1: automated discovery and inventory with owner/type/criticality. IG2: NAC/MDM/CMDB integration; auto-quarantine unknowns; alerting. IG3: near-real-time coverage including remote and cloud segments; continuous reconciliation.

Implement: Deploy discovery agents/sensors per subnet/VPC; normalize attributes; enforce device enrollment before network access; reconcile inventory daily; quarantine or enroll unknown assets automatically.

- **Evidence:** Inventory export; discovery coverage; NAC/MDM policies; tickets for unmanaged assets; daily reconciliation logs.
- **Acceptance Criteria:** Inventory coverage **≥98%** (IG2) / **≥99%** (IG3); unknown assets controlled within **24h (IG2) / 8h (IG3);** reconciliation daily; exceptions have compensating controls and expiry.
- **Common Failures:** Lab/guest/cloud sandboxes excluded; stale owners; manual spreadsheets.
- **Internal QA:** Monthly sample of 30 random assets: verify owner, enrollment, last-seen timestamp.
- **Docs:** Asset Inventory SOP; NAC/MDM Standard; CMDB Data Model.

5.2 Control 2 — Inventory and Control of Software Assets

Intent: Permit only authorized software; detect and remove unauthorized software rapidly.

Minimums: IG1: software inventory by device; basic allow-list. IG2: enforce allow-listing/script control; license tracking; alert/removal workflow. IG3: pre-deployment gating in CI/CD; runtime allow-listing on servers.

Implement: Agent-based software inventory; define authorized publishers/packages; block unauthorized executables; alert on new binaries; remove or justify within SLA; maintain exception ledger with expiry.

- **Evidence:** Software inventory exports; allow-list policy; removal tickets; exception ledger; CI/CD gate configuration.
- **Acceptance Criteria:** Coverage equals C1 asset scope; unauthorized software removed **≤5 business days (IG2) / ≤2 days (IG3)**; allow-list enforced on admin/servers.
- **Common Failures:** Local admin installs; portable binaries; exceptions without expiry.
- **Internal QA:** Quarterly rogue software hunt across 10% of fleet.
- **Docs:** Software Control Standard; Exception Procedure; CI/CD Security Gate SOP.

5.3 Control 3 — Data Protection

Intent: Classify data, enforce encryption/handling, and prevent loss/exfiltration.

Minimums: IG1: identify sensitive data types; encrypt at rest and in transit. IG2: DLP policies (email/web/endpoints), key management, data-flow mapping. IG3: data minimization for high-risk flows; monitoring of exfil channels; periodic reviews.

Implement: Define categories (e.g., customer, financial); require encryption policies on databases, filesystems, and backups; DLP policies with triage SLAs; maintain data-flow diagrams; restrict bulk export; monitor high-risk channels.

- **Evidence:** Classification policy; encryption configuration screenshots; DLP alert samples; data-flow diagrams with revision dates.
- **Acceptance Criteria:** Encryption enforced for sensitive stores and backups; DLP alerts triaged **≤1 business day (IG2) / ≤4 hours (IG3)**; annual review of categories/flows.
- **Common Failures:** Untracked SaaS exports; shared mailboxes; unencrypted backups.
- **Internal QA:** Quarterly walkthrough of three critical flows ensuring controls are active.
- **Docs:** Data Protection Standard; DLP Runbook; Encryption Standards.

5.4 Control 4 — Secure Configuration of Enterprise Assets and Software

Intent: Enforce hardened baselines; detect and remediate drift.

Minimums: IG1: baselines for OS/apps; config management. IG2: CIS Benchmark-aligned SCM with drift alerting; remediation SLAs. IG3: pre-deployment compliance checks; image attestation; signed configs.

Implement: Adopt CIS Benchmarks per platform; apply via MDM/SCM; block non-compliant builds in CI/CD; monitor drift; auto-remediate where safe; track approvals for baseline changes.

- **Evidence:** Baseline documents; SCM policies; drift reports; change approval records.
- **Acceptance Criteria:** Baseline coverage **≥95%** of managed assets; critical misconfigs remediated **≤7 days (IG2) / ≤72 hours (IG3)**; pre-deploy checks enforced.
- **Common Failures:** "Gold images" never updated; permanent exceptions.
- **Internal QA:** Monthly drift spot-check of 25 systems (server, endpoint, cloud).
- **Docs:** Secure Configuration Standard; SCM Playbook; Baseline Change SOP.

5.5 Control 5 — Account Management

Intent: Control lifecycle of user/service accounts; remove stale and shared accounts.

Minimums: IG1: Joiner/Mover/Leaver (JML) process; dormant account removal. IG2: unique service accounts with owners/rotation; SaaS identity alignment. IG3: continuous privileged monitoring; alerts for orphaned or anomalous use.

Implement: HR-driven provisioning/deprovisioning; daily reconciliation; disable dormant accounts (e.g., 30 days inactivity); service account registry with purpose/owner/rotation.

- **Evidence:** JML SOP; deprovision reports; dormant closure tickets; service account inventory; rotation logs.
- **Acceptance Criteria:** Terminated users disabled ≤24 hours; dormant users disabled weekly; service accounts documented and rotated per policy.
- **Common Failures:** Shared admin; unmanaged SaaS identities; orphaned service accounts.
- **Internal QA:** Quarterly privileged access recertification with attestation.
- **Docs:** Account Management Standard; Service Account Guide; Access Recert SOP.

5.6 Control 6 — Access Control Management

Intent: Enforce least privilege and strong authentication.

Minimums: IG1: MFA for admin and remote access; role-based access. IG2: MFA for sensitive apps; just-in-time (JIT) elevation; quarterly access reviews. IG3: continuous monitoring of privileged activity; break-glass governance.

Implement: Enforce MFA at IdP/app; remove standing admin; implement JIT; quarterly reviews; monitor break-glass with alerts.

- **Evidence:** MFA coverage reports; role catalogs; review records; JIT logs.
- **Acceptance Criteria:** MFA: admin/remote 100%; sensitive apps ≥95% (IG2) / 100% (IG3); JIT approvals logged; break-glass use alerted within minutes.
- **Common Failures:** Legacy apps without MFA; stale elevated roles; unmanaged emergency accounts.
- **Internal QA:** Monthly break-glass test and alert verification.
- **Docs:** Access Control Policy; Privileged Access SOP; MFA Standard.

5.7 Control 7 — Continuous Vulnerability Management

Intent: Identify and remediate vulnerabilities in time-bound, risk-based fashion.

Minimums: IG1: authenticated scanning; patch SLAs by severity. IG2: risk scoring (exposure/exploitability), exception ledger with expiry, verification scans. IG3: agent + image/container scanning; continuous cloud posture checks.

Implement: Weekly authenticated scans; agents on endpoints/servers; Critical/High SLAs (e.g., 7/15 days); integrate threat intel; verify remediations; maintain exceptions with compensating controls and expiry.

- **Evidence:** Scan reports; SLA trend dashboards; remediation tickets; re-scan proof; exception ledger.
- **Acceptance Criteria:** SLA adherence ≥90% (IG1/2) / ≥95% (IG3); exceptions tracked with expiry; zero unauthenticated critical external exposures.
- **Common Failures:** Scan gaps (macOS/remote/cloud); “accepted risk” forever; no verification scans.
- **Internal:** QA Monthly re-scan of 10% closed Critical/High items.
- **Docs:** Vulnerability Management Standard; Exception Ledger SOP.

5.8 Control 8 — Audit Log Management

Intent: Centralize, protect, and analyze logs for detection and investigations.

Minimums: IG1: enable and centralize logs; protect integrity. IG2: time sync; parsing/normalization; alerting; retention. IG3: immutability/WORM for critical logs; end-to-end validation drills.

Implement: Onboard OS/auth/app/cloud logs; secure storage with role-based access and immutability where feasible; define high-value alerts (auth anomalies, privilege use, new admin creation, policy changes).

- **Evidence:** Onboarding matrix; retention configs; alert samples; integrity/tamper settings; time-sync evidence.
- **Acceptance Criteria:** Coverage ≥95% of required sources; critical alerts route to on-call; clock skew within policy.
- **Common Failures:** Logs enabled but not forwarded; retention untested; no immutability for crown-jewel trails.
- **Internal QA:** Quarterly generate→collect→alert drill on three critical sources.
- **Docs:** Logging Standard; SIEM Runbook; Time Sync Policy.

5.9 Control 9 — Email and Web Browser Protections

Intent: Reduce phishing, malicious attachments, and web-borne threats.

Minimums: IG1: email filtering; browser hardening. IG2: attachment sandboxing; URL rewriting; SPF/DKIM/DMARC enforcement; block risky file types. IG3: browser isolation for high-risk roles; targeted protections for VIPs/support staff.

Implement: Configure gateway filtering/sandbox; managed browser policies; domain protections; content filtering; stricter profiles to high-risk users.

- **Evidence:** Gateway/sandbox policies; DMARC policy state; block lists; simulation reports.
- **Acceptance Criteria:** DMARC enforcement; attachment sandboxing active; high-risk file types blocked enterprise-wide.
- **Common Failures:** VIP exemptions; unmanaged browsers; stale allow-lists.
- **Internal QA:** Quarterly phishing simulation with trend tracking and targeted coaching.
- **Docs:** Email/Web Protection Standard; Browser Policy.

5.10 Control 10 — Malware Defenses

Intent: Prevent/detect malware at endpoints and servers.

Minimums: IG1: modern EDR/AV deployed. IG2: tamper protection; real-time protection; central management and alerting. IG3: behavior analytics; containment automation; scripted threat-hunting.

Implement: Roll out EDR agents with tamper protection; tune detections; integrate with IR playbooks.

- **Evidence:** Coverage report; detection and response logs; tuning changes.
- **Acceptance Criteria:** EDR healthy coverage ≥98%; critical detections alerted ≤15 minutes; response playbooks executed and recorded.
- **Common Failures:** Disabled agents; no tamper protection; exceptions without expiry.
- **Internal QA:** Weekly coverage reconciliation vs asset inventory.
- **Docs:** Endpoint Security Standard; EDR Operations Guide.

5.11 Control 11 — Data Recovery

Intent: Back up critical data/configurations; prove restores.

Minimums: IG1: scheduled backups; periodic restore tests. IG2: offline/immutable copies; defined RTO/RPO; tested restore procedures. IG3: segmented backup networks; periodic full-system restore drills.

Implement: Define tiers and RTO/RPO; run backups; verify immutable/offline copies; execute restore tests; capture results and improvements.

- **Evidence:** Backup job reports; immutable storage settings; restore logs; drill AARs.
- **Acceptance Criteria:** Quarterly successful restores for critical systems; immutable/offline copies present and tested.
- **Common Failures:** Missing configs/keys; restores untested; over-privileged backup admins.
- **Internal QA:** Random critical system restore each quarter with documented results.
- **Docs:** Data Recovery Standard; Restore Runbook; Backup Architecture.

5.12 Control 12 — Network Infrastructure Management

Intent: Harden and manage network devices with versioned configurations.

Minimums: IG1: baseline configs; inventory. IG2: secure management channels; config version control; disable unused services; NTP/AAA. IG3: signed configs; continuous compliance checks; infrastructure-as-code.

Implement: Maintain baseline templates; apply via automation; track/approve changes; review diffs regularly.

- **Evidence:** Baselines; version control logs; change approvals; compliance reports.
- **Acceptance Criteria:** Baselines applied to 100% managed devices; changes approved and recorded; critical drift remediated promptly.
- **Common Failures:** Ad-hoc CLI changes; missing backups of configs.
- **Internal QA:** Monthly config diff audit across representative devices.
- **Docs:** Network Config Standard; Change Management SOP.

5.13 Control 13 — Network Monitoring and Defense

Intent:: Visibility and detections across north-south and east-west traffic, including cloud.

Minimums: IG1: flow logs or basic IDS. IG2: tuned detections mapped to attack paths; response integration. IG3: coverage of cloud VPCs; TLS inspection as appropriate; anomaly detection.

Implement: Enable flow logs; deploy IDS/NDR; define detection catalog; integrate with IR; review MTTA/MTTR trends.

- **Evidence:** Detection catalog; alert stats; incident links; tuning records.
- **Acceptance Criteria:** Detections on credential abuse, lateral movement, C2, exfiltration; MTTA/MTTR tracked and improving.
- **Common Failures:** No cloud coverage; encrypted traffic blind spots without compensating telemetry.
- **Internal QA:** Quarterly detection efficacy tests using benign simulations.
- **Docs:** Network Monitoring Standard; Detection Engineering Guide.

5.14 Control 14 — Security Awareness and Skills Training

Intent: Build security skills and reduce risky behavior.

Minimums: IG1: annual program; phishing simulations. IG2: role-based training; risk-triggered refreshers. IG3: targeted curricula for high-risk roles; coaching loops.

Implement: Assign curricula by role; schedule simulations; track completion; coach repeat clickers; report trends.

- **Evidence:** Completion reports; assessment scores; simulation results.
- **Acceptance Criteria:** Completion ≥98%; phishing failure trending down quarter-over-quarter.
- **Common Failures:** One-and-done training; no follow-up after incidents.
- **Internal QA:** Quarterly cohort analysis and targeted interventions.
- **Docs:** Security Training Plan; Phishing Simulation SOP.

5.15 Control 15 — Service Provider Management

Intent: Ensure providers meet security requirements and notify you of incidents/changes.

Minimums: IG1: provider inventory; minimum requirements. IG2: responsibility matrices; incident/change notice SLAs; security clauses; log export rights. IG3: telemetry/evaluation rights; periodic reviews; offboarding steps.

Implement: Due diligence; contract clauses; responsibility matrix per provider; define notice channels/SLAs; schedule reviews; enforce offboarding.

- **Evidence:** Responsibility matrices; attestations; notices and handling tickets; review minutes.
- **Acceptance Criteria:** Matrices current; notices acted within SLA; periodic reviews documented; offboarding artifacts present.
- **Common Failures:** No telemetry/export rights; unclear responsibilities; poor offboarding.
- **Internal QA:** Quarterly review of top providers; sample one offboarding annually.
- **Docs:** Service Provider Standard; Responsibility Matrix Template.

5.16 Control 16 — Application Software Security

Intent: Integrate security into software lifecycle; release trustworthy builds.

Minimums: IG1: basic security requirements; dependency updates. IG2: SAST/DAST/SCA; security gates; threat modeling for critical apps. IG3: tests-as-code; signed builds; SBOM; runtime protections.

Implement: Secure SDLC; scanners in CI; severity-based fix SLAs; enforce release gates; sign artifacts; maintain SBOMs.

- **Evidence:** Pipeline configs; scan results; release approvals; SBOM repo; signature verification logs.
- **Acceptance Criteria:** Critical vulns remediated pre-release or excepted with expiry; SBOM for critical apps; signed builds enforced.
- **Common Failures:** Findings accepted near release with no expiry; unsigned artifacts.
- **Internal QA:** Quarterly re-performance on one critical app (rerun scans; verify gates).
- **Docs:** AppSec Standard; Release Gate SOP; SBOM Procedure.

5.17 Control 17 — Incident Response Management

Intent: Prepare, detect, respond, recover, and learn.

Minimums: IG1: IR plan; contacts; tabletop. IG2: severity scheme; playbooks; metrics (MTTA/MTTR). IG3: integrated comms (PR/Legal); third-party engagement; forensics readiness.

Implement: Define roles; maintain playbooks; test via tabletops; measure/report metrics; capture actions and verify effectiveness.

- **Evidence:** IR plan; tabletop AARs; incident timelines; metric reports; action tracker.
- **Acceptance Criteria:** ≥2 tabletops/year; actions tracked to closure with evidence; metrics trending favorable or explained.
- **Common Failures:** No measurable follow-through; outdated contacts.
- **Internal QA:** Post-incident metric review and control updates.
- **Docs:** IR Plan; Playbooks; AAR Template; Communications Plan.

5.18 Control 18 — Penetration Testing

Intent: Validate defenses by planned testing and drive remediation.

Minimums: IG1: scoped external test annually. IG2: internal, cloud, and application testing; retests. IG3: adversary emulation/purple-team; threat-led testing.

Implement: Annual scope aligned to risks; prioritize crown jewels; ensure remediation tickets and retests; record lessons learned.

- **Evidence:** Test scopes; reports; retest proofs; remediation tickets and closure.
- **Acceptance Criteria:** High/Critical findings remediated or excepted with expiry; retests passed; decreasing repeat findings.
- **Common Failures:** No retest; recurring identical weaknesses.
- **Internal QA:** Track repeats and escalate in Management Review.
- **Docs:** Penetration Testing Policy; Remediation SOP.

5.19 Applied Narrative A (IG1 rollout of core safeguards)

A business unit with laptops and SaaS apps: discovery detects all devices within two weeks; unknowns quarantined until enrolled in MDM and EDR. Baselines applied; drift alerts open tickets. Admin/remote MFA is universal. Logs from IdP, endpoints, and SaaS admin events feed SIEM; critical rules alert to on-call. Backups protect workstation profiles; a restore test succeeds. An internal audit samples 30 assets and verifies owners, enrollment, and drift remediation. Two exceptions (legacy app without MFA; one device model delay for EDR) are approved with compensating controls and 30-day expiry.

5.20 Applied Narrative B (IG3 internet-facing workload)

A high-traffic API in cloud: network configs are templated and versioned; IDS/NDR covers VPCs with flow logs analyzed. CI pipelines enforce SAST/SCA/DAST; builds are signed and SBOMs stored. Weekly agent scans plus image/container scanning meet 7/15-day SLAs; two exceptions use WAF rules and have 14-day expiry. Control-plane and workload logs are centralized with WORM for audit trails. IR tabletop simulates API abuse; fixes reduce MTTA by 35%. Annual pen-test plus cloud-specific assessments remediates Highs; retest confirms closure.

Apptega

6. Organization-Defined Parameters (ODPs) & Metric Definitions

Document components, interfaces, trust zones, external services, and where CJI flows, rests, and leaves. Maintain records of processing (sources, stores, transmissions, recipients). Update upon material change. Include the diagram and narrative in the SSP by Day 15; keep synchronized through the Day-45 full draft and pre-audit freeze.

Parameter	IG1 Target	IG2 Target	IG3 Target	Owner	Review Cadence
Asset inventory coverage	≥95%	≥98%	≥99%	ITAM Lead	Monthly
Unknown asset time-to-control	≤24h	≤12h	≤8h	SecOps	Weekly
Unauthorized software removal	≤10d	≤5d	≤2d	SecOps	Weekly
Patch SLA (Critical/High)	14d/30d	7d/15d	7d/15d (risk-adjusted)	SecOps	Weekly
EDR healthy coverage	≥95%	≥98%	≥99%	SecOps	Weekly
MFA coverage (admin/remote)	100%	100%	100%	IAM Lead	Monthly
Log coverage (required sources)	≥90%	≥95%	≥98%	SecOps	Monthly
Restore tests (critical systems)	1/qtr	3/qtr	5/qtr	IT Ops	Quarterly
Phishing failure rate	<8%	<5%	<3%	L&D	Quarterly
Pen-test remediation (High/Crit)	≤60d	≤45d	≤30d	Red Team	Quarterly

Metric definitions: Inventory Coverage %, Unknown Asset Time-to-Control, Patch SLA Adherence %, EDR Healthy Coverage %, Log Coverage %, Restore Success %, Phishing Failure %, Pen-test Remediation Timeliness % — defined exactly as previously rendered.

Apptega

6A. Metrics & Evidence Map

Metric (KRI/KPI)	CIS Outcome Supported	Source System	Owner	Evidence Location	Review
Inventory Coverage %	C1 good state	Discovery + ITAM	ITAM Lead	Sec/Inventory/	Monthly
Unauthorized SW Removal SLA	C2 good state	EDR/Endpoint Mgmt	SecOps	Sec/Software/	Weekly
Patch SLA Adherence	C7 good state	Vuln Mgmt	SecOps	Sec/Vuln/	Weekly
Log Coverage %	C8 good state	SIEM	SecOps	Sec/Logging/	Monthly
Restore Success %	C11 good state	Backup Platform	IT Ops	Sec/Recovery/	Quarterly
MFA Coverage %	C6 good state	IdP + apps	IAM Lead	Sec/MFA/	Monthly
EDR Healthy Coverage %	C10 good state	EDR console	SecOps	Sec/EDR/	Weekly
DMARC Enforcement	C9 good state	Email gateway/DNS	SecOps	Sec/MailWeb/	Quarterly
Phishing failure rate	<8%	<5%	<3%	L&D	Quarterly
Pen-test remediation (High/Crit)	≤60d	≤45d	≤30d	Red Team	Quarterly

6B. Exception Governance Policy (Time-Boxed with Compensating Controls)

- **Required fields:** Gap description, impacted environments, risk statement, compensating controls, owner, approver, expiry date, evidence link.
- **Max expiry by risk:** High ≤30 days; Medium ≤90 days; Low ≤180 days.
- **Compensating controls (choose ≥2):** Increased monitoring/alerting; reduced exposure (segmentation/ACL/WAF); accelerated remediation SLA; additional approvals; targeted training.
- **Renewals:** One renewal allowed with new justification; second renewal requires executive approval.
- **Reporting:** All active exceptions reviewed at each Management Review; ledger shows status and next steps.

Apptega

7. Evidence Register (Authoritative Artifacts)

(Locations, owners, formats, and review dates listed exactly as in the last full version; retained here for completeness.)

Artifact	Control(s)	Location/Path	Owner	Format	Last Updated	Verifier	Next Review
Asset inventory & discovery coverage	C1	Sec/Inventory/	ITAM Lead	CSV/PDF			
Software inventory & allow-list	C2	Sec/Software/	SecOps	CSV/PDF			
Data classification, encryption, DLP	C3	Sec/Data/	Data Owner	PDF/CSV			
Baselines & drift reports	C4	Sec/Baselines/	Platform Eng	PDF/CSV			
JML & dormant/service account reports	C5	Sec/Identity/	IAM Lead	PDF/CSV			
MFA coverage & access reviews	C6	Sec/MFA/	IAM Lead	CSV/PDF			
Vuln scans, SLA trends, exceptions	C7	Sec/Vuln/	SecOps	PDF/CSV			
Log onboarding matrix & alerts	C8	Sec/Logging/	SecOps	PDF/CSV			
Email/web protections & DMARC	C9	Sec/MailWeb/	SecOps	PDF			
EDR coverage & detections	C10	Sec/EDR/	SecOps	PDF/CSV			
Backup plans & restore evidence	C11	Sec/Recovery/	IT Ops	PDF/CSV			
Network baselines & changes	C12	Sec/Network/	NetEng	PDF/CSV			
Detection catalog & MTTA/MTTR	C13	Sec/Detect/	SecOps	PDF/CSV			
Training & phishing results	C14	Sec/Training/	L&D	PDF/CSV			
Provider matrices & notices	C15	Sec/TPRM/	TPRM Lead	PDF/ XLSX			
SDLC gates, scans, SBOMs	C16	Sec/AppSec/	AppSec	PDF/CSV			
IR plan, AARs, actions	C17	Sec/IR/	IR Lead	PDF/CSV			
Pen-test reports & retests	C18	Sec/Pentest/	Red Team	PDF			

8. Continuous Monitoring (KRIs, Alerts, Automation)

KRIs, thresholds, owners, and auto-actions are exactly as rendered previously (unmanaged asset count, EDR healthy coverage, MFA gaps, patch SLA breaches, log ingestion failures, backup restore failures). Automation: daily asset reconciliation; auto-ticket on threshold breach; CI/CD blocks for non-compliant baselines; NAC quarantine for unknown devices; monthly WORM verification job.

8A. Quarterly Operating Calendar

- **Week 1:** Inventory reconcile; EDR gap sweep; log source health check.
- **Week 2:** Patch SLA review; exception ledger review (upcoming expiries).
- **Week 3:** Log E2E drill (generate→collect→alert); restore test (one critical system).
- **Week 4:** Provider tier review (top vendors); phishing simulation or targeted training.
- **Quarterly:** Internal audit slice; Management Review (decisions/actions recorded).
- **Annually:** Pen-test cycle; policy refresh; IG re-scoring.

9. Internal Audit Program (CIS v8.1)

- **Plan:** Q1 C1–C4 • Q2 C5–C8 • Q3 C9–C14 • Q4 C15–C18.
- **Method:** Interviews; document review; re-performance (restore test, detection test); sampling ≥10 items or ≥10%; verify CAPA effectiveness.
- **Acceptance:** Plan executed; majors closed on time; recurrence trending down.

10. Management Review (Security Governance)

- **Inputs:** IG status and ODPs; KRI trends; audit findings; incidents/AARs; provider notices; exception ledger with **expiry**; resourcing asks.
- **Outputs:** Decisions and actions with owners/dates; risk acceptances with expiry; funding assignments; policy updates.
- **Cadence:** Semiannual minimum; additionally after major incident or material change.
- **Acceptance:** 100% actions closed or extended (justified) by next review.

10A. Management Review Pack (What to Bring)

- ODP dashboard with trend lines and red/yellow items.
- Exception ledger sorted by expiry (next 60 days).
- Top 10 risk-prioritized backlog items and status.
- Provider notices since last review and actions taken.
- Audit findings aging report (open Major/Minor, due dates).
- Funding/resource asks with impact statement.

11. Corrective Action (RCA/CAPA) Workflow

- Detect → Contain → RCA → Action Plan (owner/date) → Implement → Verify effectiveness (metric improved/retest) → Close → Update docs/training.
- **Timelines (example):** Major verify ≤30 days; Medium ≤45 days; Low ≤60 days.
- **Effectiveness examples:** Patch SLA 82%→96%; EDR coverage 95%→99%; MTTA down 40% for repeated alert type.

12. Change Management for Security-Impacting Changes

- **Triggers:** Changes to baselines (C4), identity/MFA (C6), logging scope (C8), network exposure (C12–C13), backup architecture (C11), provider scope (C15), and SDLC gates (C16).
- **Pre-change gates:** Impact analysis, approvals, rollback plan, pilot results, comms/training.
- **Post-change checks:** Validate ODPs; confirm monitoring; capture evidence.

12A. Change-Impact Matrix (When Extra Checks Apply)

- **Increased internet exposure** → update detections, review log scope, schedule focused pen-test.
- **Baseline changes** → staged rollout + drift monitoring, rollback plan, doc update.
- **Identity/MFA changes** → break-glass test and access review within 14 days.
- **Backup architecture changes** → restore test within 7 days.

13. Evidence Sampling Plans (Internal QA)

- **C1/C2:** random 30 assets quarterly;
- **C7:** re-scan 10% of closed Critical/High monthly;
- **C8:** end-to-end drills for three critical sources quarterly;
- **C11:** restore one to five critical systems quarterly (per IG);
- **C15:** review two provider matrices + last notice each quarter;
- **C16:** re-perform security gates on one critical app quarterly.

14. Common Pitfalls & Anti-Patterns

Discovery gaps (guest/lab/cloud); MFA carve-outs without expiry; EDR agents disabled or tamper-off; logs enabled but not centralized; patch SLAs without owners; provider contracts lacking notice/telemetry rights; exceptions that never expire.

15. Cloud & Hosting Scenarios — CIS Shared-Responsibility Mapping

Area	SaaS	IaaS/PaaS (cloud)	On-Prem
Asset/Software Inventory	SSO discovery; admin audit logs	Cloud inventory + agents/ images	ITAM + agents
Secure Configuration	Admin policies; vendor features	CSPM + hardening baselines	GPO/MDM/SCM
Vulnerability Mgmt	Vendor advisories & config checks	Agents + image/container scans	Authenticated scans
Audit Logs	Admin/audit export to SIEM	Cloud logs + SIEM (WORM for critical)	Syslog/SIEM
Malware Defenses	Endpoint at client side	Agents for workloads	EDR/AV endpoints
Data Recovery	Vendor retention/export	Snapshots + backups + immutability	Traditional backups
Provider Management	C15 clauses + notices	C15 clauses + notices & telemetry	N/A

Acceptance: Responsibility matrix exists per scenario; monitoring ownership and evidence paths are explicit.

15A. Service Provider Tiering & Minimums

- **Tier 1 (crown-jewel):** Telemetry/export rights; incident/change notice ≤24h; annual security review; documented vulnerability/patch expectations; log retention export; right to independent assurance.
- **Tier 2:** Notice ≤72h; evidence of vulnerability management; admin audit logs export.
- **Tier 3:** Basic security terms; admin access controls; termination/offboarding requirements.
- Maintain a Provider Responsibility Matrix (You / Provider / Shared) covering inventory, configuration, vulnerability mgmt, logging, backups, incident/change notices.

16. Evidence & Documentation Checklist

CIS adoption & IG targets; asset & software inventories (coverage reports); baselines & drift reports; MFA/access policies and reviews; vulnerability scans/SLA trends/ exception ledger; log onboarding matrix, alerts, retention; EDR coverage/detections; backup plans & restore test results; network baselines & change logs; training completion & phishing trends; provider matrices & notices; IR plan/AARs/metrics; pen-test reports & retests.

17. Training & Competence (Role Rubrics)

Role	Must Demonstrate	Assessment
SecOps	EDR admin; SIEM queries; vuln tool use	Lab practical + quiz
IAM	MFA policies; RBAC/JIT; access reviews	Access recert walkthrough
Platform/Cloud	Baselines; CSPM; hardening	Pipeline/live demo
NetEng	Device baselines; segmentation; ACLs	Config diff review
AppSec	SAST/DAST/SCA; release gates; SBOM	Pipeline artifacts review
IR	Severity triage; playbooks; comms	Tabletop facilitation
TPRM	Security clauses; matrices; notice handling	Contract/matrix review

Targets: ≥98% completion; ≥85% pass for critical roles; repeat findings trending down.

17A. Role Onboarding Kit (First 3 Tasks)

- **SecOps:** Gain SIEM/EDR/vuln tool access; run EDR coverage report; schedule first log E2E drill.
- **IAM:** Review MFA coverage; test break-glass; schedule next access review.
- **NetEng:** Export baseline compliance; review config diffs; submit remediation plan for top 3 gaps.
- **AppSec:** Validate CI scanners; review last SBOM; verify release gates.
- **IR:** Tabletop schedule; update contact roster; run paging test.
- **TPRM:** Update top vendor matrices; verify notice channels; confirm next review dates.

18. FAQs (Executives & Auditors)

- **Proving IG1:** Show inventories, secure baselines, MFA (admin/remote), EDR coverage, centralized logging, backup/restore proof, and one tabletop.
- **Raising to IG2/IG3:** Prioritize internet-facing and crown-jewel systems; raise ODP targets; expand detections and testing.
- **Most useful evidence:** Coverage & SLA trends, alert samples, restore proofs, retest confirmations, exception expiries.

19. Self-Assessment & Leadership Attestation

Track per control: Status (C/PC/NC), owner, evidence link, action ID and due date. Leadership attests that scope/IG declarations are accurate; “C” entries have current evidence; PC/NC items have owners and dates; exceptions carry compensating controls and expiry.

Signature

Name/title

Date

19A. Self-Assessment Survey (C/PC/NC Quick Scan)

1. Do we have ≥98% asset inventory coverage (or our ODP target) across all IG2+ environments?
2. Are unknown assets quarantined or enrolled within our ODP time?
3. Is software allow-listing enforced on admin workstations and servers?
4. Are Critical/High vulnerabilities meeting our SLA adherence targets?
5. Do we have ≥95% log coverage of required sources with tested alerts?
6. Is EDR healthy coverage meeting our ODP?
7. Have we successfully restored at least one critical system this quarter?
8. Are MFA gaps for admin/remote access at 0%?
9. Do all active exceptions have compensating controls and a future expiry date?
10. Have we completed ≥2 IR tabletops this year and tracked corrective actions?
11. Do Tier 1 providers meet telemetry/export and 24h notice minimums?
12. Were High/Critical pen-test findings remediated or excepted with expiry within target?

20. References

Center for Internet Security. CIS Controls v8.1. 2024
https://www.cisecurity.org/controls/cis-controls

Center for Internet Security. CIS Controls v8.1 — Implementation Groups (IG1–IG3) Guidance 2024.
https://www.cisecurity.org/insights/white-papers/implementation-groups

Center for Internet Security. CIS Benchmarks (Platform Hardening Benchmarks) 2025
https://www.cisecurity.org/cis-benchmarks

21. Minimal Policy Set

1. Enforce MFA for all administrative and remote access.
2. Maintain automated asset and software inventories; block unmanaged/ unauthorized items.
3. Apply and monitor secure configuration baselines prior to deployment.
4. Operate risk-based vulnerability management with time-bound SLAs and expiring exceptions.
5. Centralize and protect audit logs with alerting and defined retention.
6. Deploy EDR with tamper protection and verify coverage.
7. Perform regular backups and prove restores for critical systems.
8. Maintain network baselines with version control and approved changes.
9. Operate security awareness and skills training with behavior measurement.
10. Manage service providers with tiered minimums, notices, and telemetry or export rights.
11. Integrate security into software delivery with gates and signed releases.
12. Run incident response with metrics and after-action improvements.
13. Conduct planned penetration testing with remediation and retest.

22. Communications Plan & Templates

- **What gets communicated:** IG changes; exception expiries; provider notices; incident learnings; quarterly performance highlights.
- **Who communicates:** GRC (program status); SecOps/IAM/NetEng/AppSec (contro status); IR (incidents/AARs); TPRM (provider notices).
- **Channels:** Email to control owners; quarterly exec readout; wiki updates; SIEM dashboards.

Template — Exception Expiry Reminder (≤14 days)

Subject: [Action Required] Exception {ID} expires on {Date}

Body: This exception for {Control/Gap} expires on {Date}. Compensating controls: {List}. Owner: {Name}. Please remediate or submit renewal justification. Unaddressed expiries will trigger block/alternate control within 48 hours.

Template — Provider Incident Notice (Tier 1)

Subject: Provider Incident Notice – {Vendor} on {Date}

Body: {Vendor} reported {incident/change}. Impacted services: {List}. Our actions: {Monitoring/Controls}. Evidence location: {Path}. Next update: {Date/Time}.

Template — Quarterly Program Highlights

Subject: Security Program Quarterly Highlights (CIS v8.1)

Body: KPIs (ODPs): {Top metrics}. Completed: {Audits, Drills}. Open risks: {Top 3}. Exceptions expiring next 30 days: {IDs}. Decisions needed: {Bullets}.

Annex A — Control→Safeguard Mapping (IG1/IG2/G3 selection)

Maintain your authoritative list of selected Safeguards per Control and IG with links to procedures and evidence. Include an “Exceptions with Expiry” column. Update after environment or IG changes.

Annex B — Sample Auditor Evidence Pack (CIS v8.1)

Topic	Primary Artifacts	Suggested Sample
C1/C2 Inventories	Inventory exports; coverage reports	All IG2/IG3 envs + 2 IG1
C4/C7 Baselines & Patching	Baselines; drift & SLA trend; exceptions	Last 90 days
C6 Access	MFA coverage; access review records	Last 2 quarters
C8 Logging	Onboarding matrix; alert samples; WORM proof	3 critical sources
C10 EDR	Coverage; detection/response logs	All servers + VIP endpoints
C11 Recovery	Restore test evidence; immutable storage	2–5 critical systems
C15 Providers	Responsibility matrices; recent notices	Top 3 vendors
C17/C18 IR & Pen Test	IR plan, AARs, metrics; pen-test & retest	Latest cycle

Annex C — Templates

Exception & Compensating Controls Ledger

ID	Control	Gap	Compensating Control	Approver	Start	Expiry	Owner	Evidence	Status

Risk Acceptance Form

Field	Entry
Control / Safeguard	
Risk description & business context	
Residual risk & justification	
Expiry / Review date	
Approver (role/name)	
Evidence/links	

Service Provider Responsibility Matrix

Area	You	Provider	Shared	Evidence
Vulnerability mgmt				
Logging/export				
Incident/change notice				
Configuration/hardening				
Backup/retention				

Apptega

Apptega Product Features

16+ Security Frameworks

One-Click Reporting

Automated Alerts & Notifications

API & Application Connectors

Automated Framework Crosswalking

Real-Time Compliance Scoring

Restricted Auditor View

Single Sign-On Connectivity

Policy & Plan Templates

Automated Risk Assessments

Document Repository for Artifacts

Multi-Tenant Environment

Apptega

About Apptega

A perennial G2 leader across various cybersecurity categories, Apptega is the cybersecurity and compliance platform purpose-built for security providers who are growing lucrative security practices, creating stickier customer relationships, and winning more business from competitors.

With Apptega's end-to-end platform, IT providers can:

1. Build continuous compliance offerings that set them apart, retain customers, and grow their ARR.
2. Build and manage world-class cybersecurity and compliance programs for their clients.
3. Increase the capacity and efficiency of their existing team so they can service 2–3× more customers.
4. Assess, measure, and manage their own security programs against a standard set of industry-leading frameworks.

To learn more, visit apptega.com

Visit apptega.com