Cloudflare Configuration Audit Checklist

BLACKHAWK DATA

DNS & SSL/TLS

- □ All DNS records proxied through Cloudflare (orange cloud)
- □ SSL/TLS mode set to Full (Strict)
- □ Origin certificate installed and valid
- □ DNSSEC enabled
- □ Minimum TLS version set to 1.2
- □ Always Use HTTPS enabled
- □ HSTS enabled with appropriate max-age

WAF & Security

- □ Cloudflare Managed Ruleset enabled and in Block mode
- □ OWASP Core Ruleset enabled
- □ Custom WAF rules for application-specific protection
- □ Rate limiting configured on authentication endpoints
- □ Bot Management enabled with score thresholds
- □ Turnstile deployed on critical forms
- □ IP allowlists reviewed and narrowed

Performance

- □ Caching rules configured for static assets
- □ Cache hit ratio above 80%
- □ Argo Smart Routing enabled (if applicable)
- □ Image optimization enabled (Polish, Resize)
- □ HTTP/3 enabled
- □ Early Hints enabled
- □ Browser cache TTL configured

Zero Trust (if applicable)

- □ Cloudflare Access policies configured per application
- □ Identity provider integrated
- □ Device posture checks enabled
- □ Gateway DNS and HTTP policies active
- □ Browser Isolation configured for high-risk sites