
Auditope

by CAI Technology

# Raport Audit

Evaluare automatizată end-to-end

https://auditope.com/

HEALTH SCORE

72

C — necesită îmbunătățiri

auditope.com

Audit ID: 2fe7cec6-c056-4b12-8d1e-46e635c31772

Generat: 20 May 2026 · 07:38 UTC

# Raport întocmit pentru

Date persoană juridică (ONRC + ANAF, snapshot la momentul auditului)

| | |
|---|---|
| DENUMIRE | CAI TECHNOLOGY S.R.L. |
| CUI | 50512457 |
| COD ÎNMATRICULARE | J2024020380005 |
| SEDIU SOCIAL | VICTOR BRAUNER, Bucureşti Sectorul 3, jud. Bucureşti, 32621 |
| REPREZENTANT LEGAL | CONSTANTIN NICUŞOR-GELU (administrator) |
| CAEN PRINCIPAL | 1812 Alte activități de tipărire n.c.a. |
| STARE FIRMĂ | funcțiune |

# Sumar executiv

Privire de ansamblu asupra stării site-ului

Site-ul auditope.com prezintă o infrastructură tehnică solidă, cu scoruri excelente la SEO și accesibilitate generală, dar suferă de vulnerabilități critice de securitate a emailului (lipsa SPF/DKIM/DMARC) și o configurație periculoasă a CSP care permite execuția de scripturi nesigure. Performanța pe mobil este afectată de timpi mari de încărcare (LCP) și blocarea main thread-ului, iar lipsa optimizării pentru citarea de către AI bots reduce vizibilitatea în noile motoare de căutare generative. Prioritățile imediate sunt remedierea headerelor de securitate, deblocarea AI bots în robots.txt și optimizarea contrastului culorilor pentru conformitate WCAG. Implementarea acestor măsuri va proteja reputația domeniului și va crește rata de conversie prin UX îmbunătățit.

## PUNCTE FORTE

- Scoruri excelente de SEO (100/100) și accesibilitate generală (96/100) pe desktop.
- Configurație robustă de fișiere statice (robots.txt, sitemap.xml, security.txt, llms.txt, ai.txt).
- Performanță optimă pe desktop (100/100) și citabilitate excelentă pentru AI (Grade A).

## DETALII AUDIT

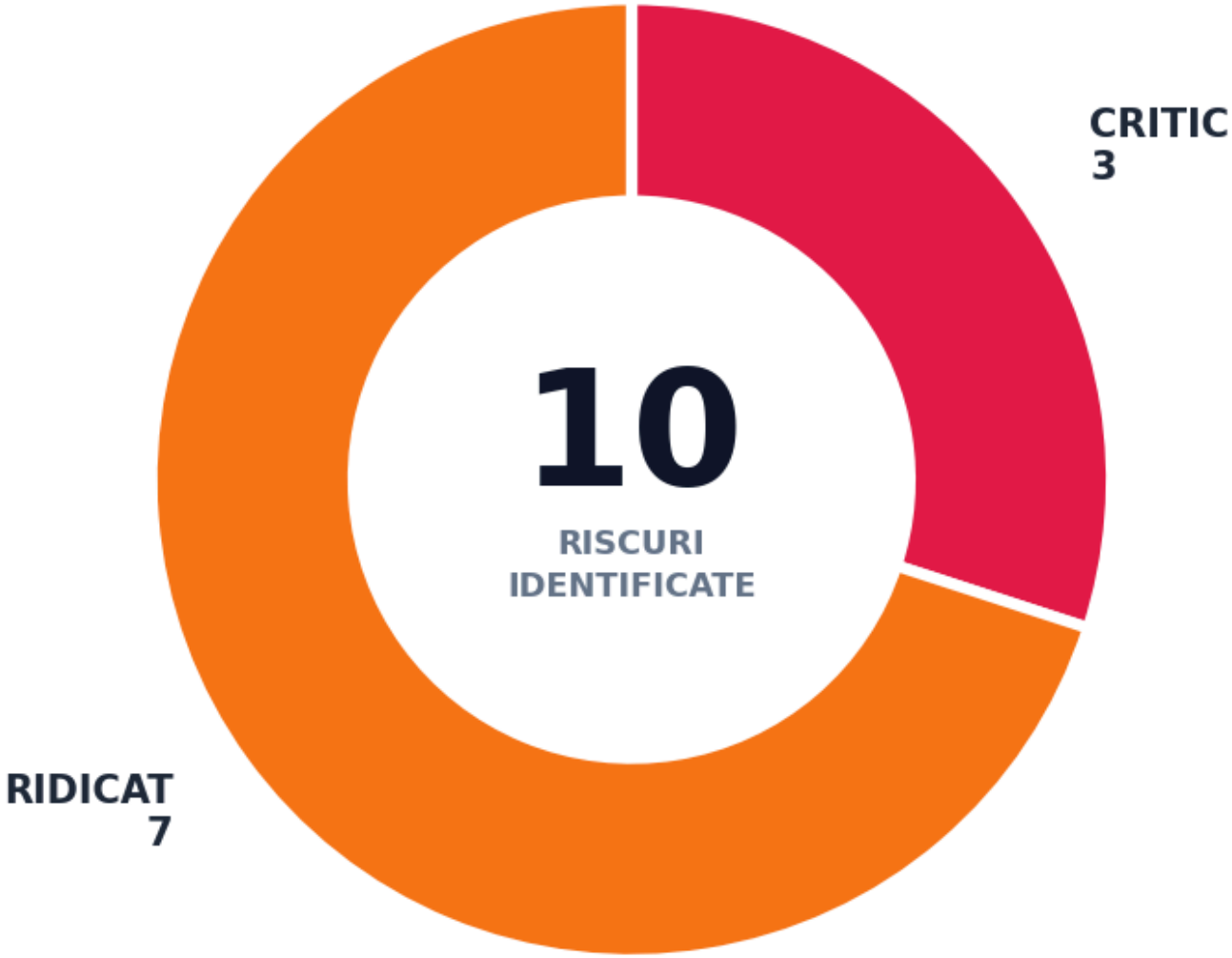
| HEALTH SCORE | FINDINGS TOTALE | ACȚIUNI PRIORITARE |
|---|---|---|
| 72/100 | 10 | 10 |

## DISTRIBUȚIE PE SEVERITATE

| CRITIC | RIDICAT | MEDIU | SCĂZUT | TOTAL |
|---|---|---|---|---|
| 3 | 7 | 0 | 0 | 10 |

## DISTRIBUȚIE VIZUALĂ RISCURI

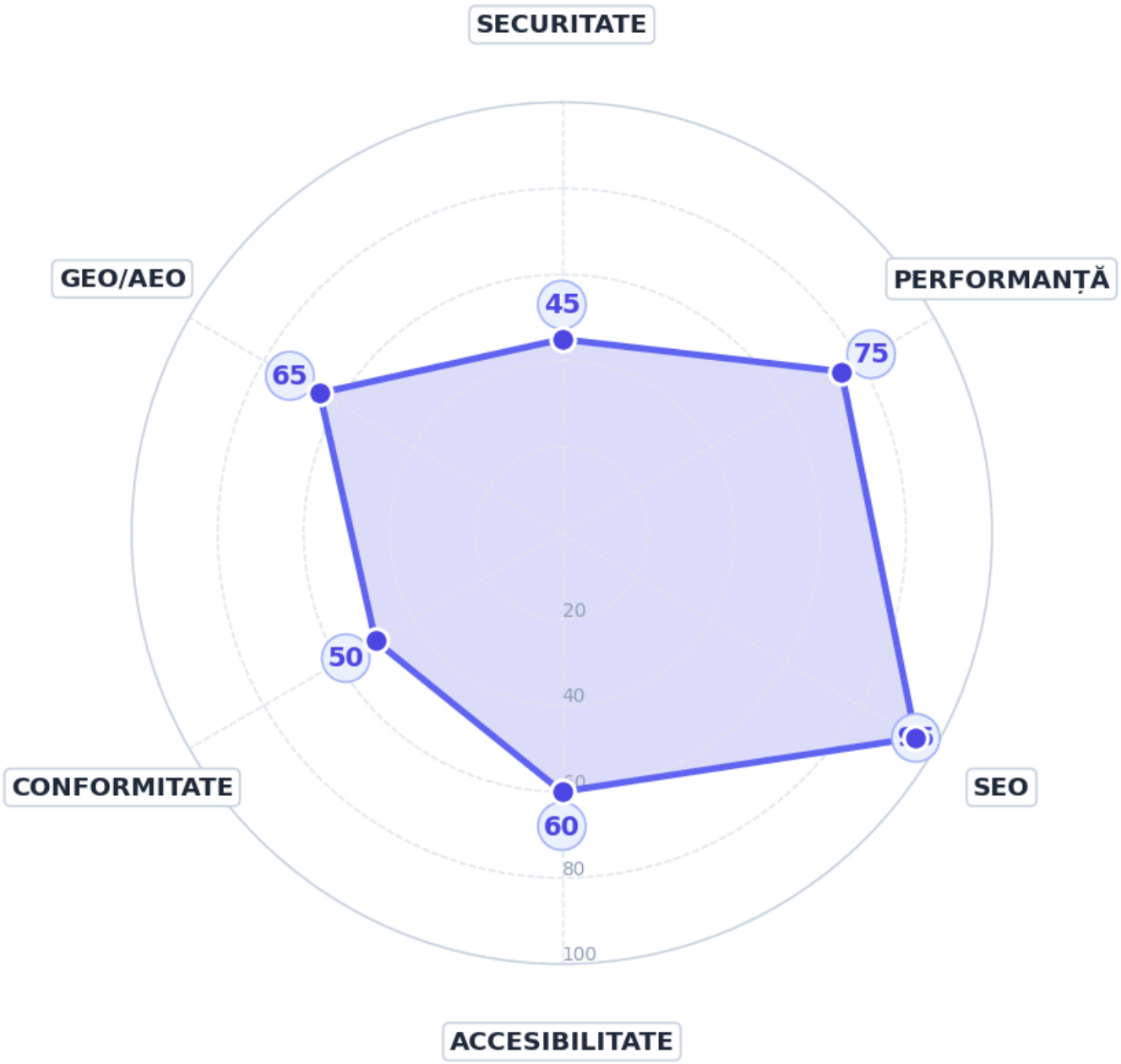
## Distribuție riscuri pe severitate



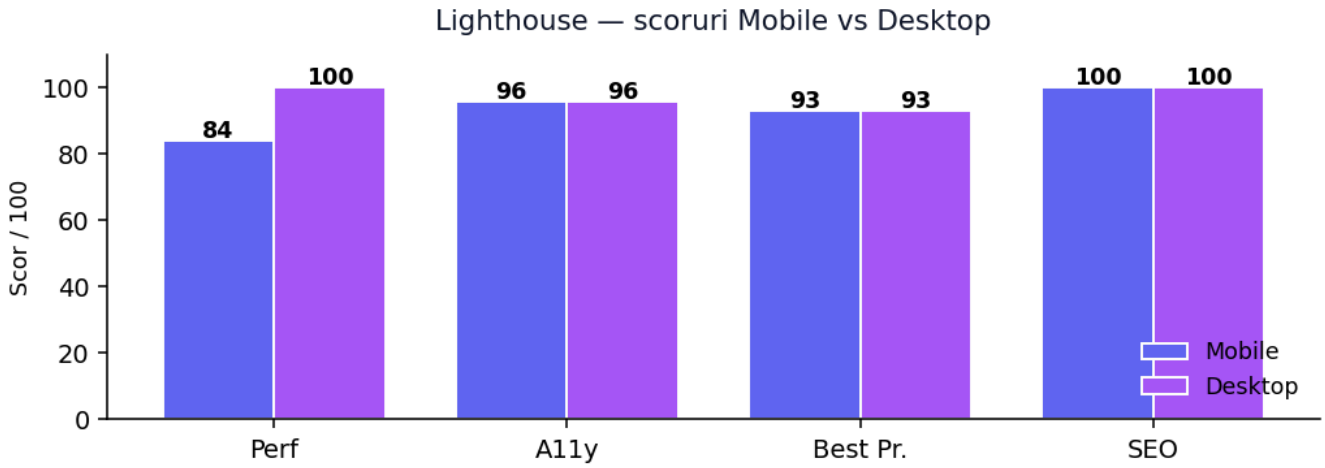
# Defalcare scor

Performanța per categorie + comparație Lighthouse mobile vs desktop

## RADAR PE CATEGORII




## COMPARAȚIE LIGHTHOUSE




## SCORURI PER CATEGORIE

| | | |
|---|---|---|
| Securitate | | 45/100 |
| Performanță | | 75/100 |
| SEO | | 95/100 |
| Accesibilitate | | 60/100 |
| Conformitate | | 50/100 |
| GEO/AEO | | 65/100 |

# Phase 01 — Probes (HTTP/TLS/DNS)

Date de bază colectate prin requesturi pure HTTP (sub 1 secundă)

## STATUS HTTP

URL final: `https://auditope.com/` (status 200)

Redirect hops: 0

Content-Type: `text/html; charset=utf-8`

Body size: 33,693 bytes

## CERTIFICAT TLS

Status: Valid

Issuer: E7 (Let's Encrypt)

Expiră în: 75 zile (`Aug 3 08:32:24 2026 GMT`)

Cipher: `TLS_AES_128_GCM_SHA256`

Versiune: `TLSv1.3`

## DNS RECORDS

| TYPE | VALUES |
|---|---|
| A | 10.11.10.84 |
| AAAA | — |
| CNAME | — |
| MX | — |
| TXT | — |
| CAA | — |

## SECURITY HEADERS

| HEADER | STATUS |
|---|---|
| strict-transport-security | ✓ prezent |

| HEADER | STATUS |
|---|---|
| content-security-policy | ✓ prezent |
| x-content-type-options | ✓ prezent |
| x-frame-options | ✓ prezent |
| referrer-policy | ✓ prezent |
| permissions-policy | ✓ prezent |

## FIȘIERE STATICE

| FIȘIER | STATUS | MĂRIME |
|---|---|---|
| /robots.txt | ✓ prezent | 2,254 B |
| /sitemap.xml | ✓ prezent | 1,603 B |
| /llms.txt | ✓ prezent | 4,714 B |
| /.well-known/security.txt | ✓ prezent | 480 B |
| /.well-known/ai.txt | ✓ prezent | 633 B |

# Phase 02 — Lighthouse

Audit Google Lighthouse (Performance + A11y + Best Practices + SEO)

## SCORURI

| CATEGORIE | MOBILE | DESKTOP |
|---|---|---|
| Performance | 84/100 | 100/100 |
| Accessibility | 96/100 | 96/100 |
| Best Practices | 93/100 | 93/100 |
| Seo | 100/100 | 100/100 |

## CORE WEB VITALS (MOBILE)

| METRIC | VALOARE | SCOR |
|---|---|---|
| FCP | 1.7 s | 92/100 |
| LCP | 2.9 s | 81/100 |
| TBT | 410 ms | 67/100 |
| CLS | 0.003 | 100/100 |
| Speed Index | 2.2 s | 99/100 |
| TTI | 3.0 s | 96/100 |

## AUDITS FAILED (TOP 20)

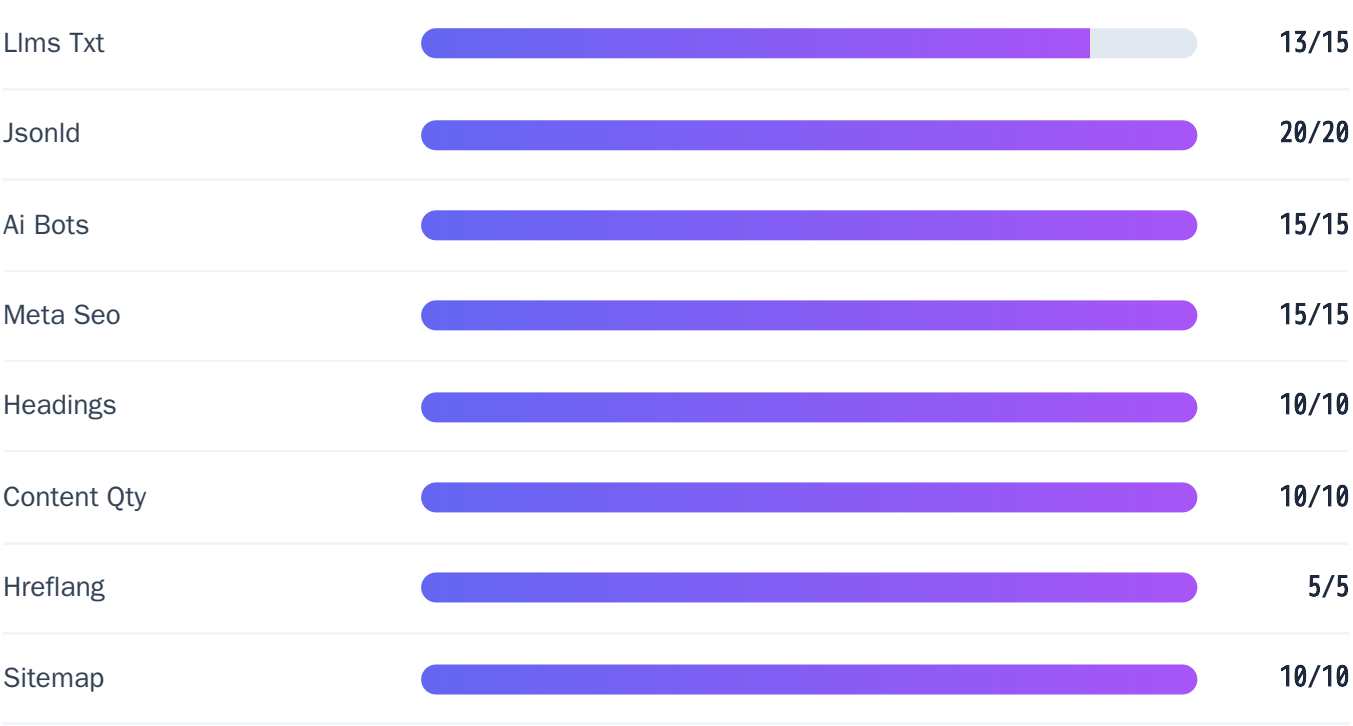
- `largest-contentful-paint`
- `total-blocking-time`
- `max-potential-fid`
- `errors-in-console`
- `color-contrast`
- `label-content-name-mismatch`
- `inspector-issues`

# Phase 04 — GEO/AEO

Pregătirea site-ului pentru a fi citat de AI engines (ChatGPT, Claude, Perplexity, Gemini, Google AI)

## SCOR CITABILITY: 98/100 — A — EXCELLENT AI CITABILITY

## DEFALCARE SEMNALE



# Mozilla Observatory · Security headers

Scoring clean room conform methodology Mozilla (zero API extern)

GRADE

B+

Mozilla Observatory score

80/100

11 teste trecute · 1 eșuate · 21 bonus

Breakdown per test

| | | |
|---|---|---|
| Csp | -20 | CSP permite 'unsafe-inline' pe script-src |
| X Content Type | 0 | X-Content-Type-Options: nosniff |
| Cookies | 0 | Niciun cookie detectat |
| Cors | 0 | CORS restricted (default — fără Access-Control-Allow-Origin) |
| Redirection | 0 | Redirect chain securizat |
| X Xss Protection | 0 | X-XSS-Protection deprecated — absent OK |
| Permissions Policy | +2 | Permissions-Policy prezent (camera/microphone restricted) |
| Co Coop | +2 | COOP prezent |
| Co Corp | +2 | CORP prezent |
| Hsts | +5 | HSTS preload-ready (max-age≥1yr + includeSubDomains + preload) |
| X Frame Options | +5 | frame-ancestors prezent în CSP (modern) |
| Referrer Policy | +5 | Referrer-Policy: strict-origin-when-cross-origin |

# Standards & Compliance Mapping

Mapează findings la standards/regulations relevante (ISO, GDPR, WCAG, OWASP, PCI-DSS, NIST)

Standards touched: 4 · 48 findings total cu mapping

| Standard / Regulation | Findings (rule_ids) | Count |
|---|---|---|
| Mozilla Web Security Guidelines | `headers-csp-issue` | 1 |
| OWASP Top 10 A05:2021 | `headers-csp-issue` | 1 |
| W3C Service Worker w3.org/TR/service-workers/ | `pwa-no-service-worker` | 1 |
| WCAG 2.2 SC 3.1.5 (AAA) | `readability-difficult` | 1 |

Sursa mapping: standards_mapping.json (Auditope v1.0 — open standards public). Mapping non-exhaustiv — verifică manual specii noi (NIS2, AI Act).

# Top acțiuni prioritare

Prioritizate după impact business × severitate × efort. Primele 3-5 fix-uri = ROI maxim.

CRITIC | SECURITATE | IMPACT 95/100 | ~10 MIN

#1

## Configure SPF Record for Email Authentication

📋 RECOMANDARE (TL;DR)

Add a TXT DNS record `v=spf1 mx -all` (or include your provider like Google Workspace) to prevent email spoofing and ensure legitimate emails reach the inbox.

⚠ RISC BUSINESS & IMPACT

Fără SPF, atacatorii pot spoofa domeniul dvs. pentru campanii de phishing, ducând la pierderea încrederii clienților și blocarea domeniului de către providerii de email. Conform GDPR Art. 32, lipsa măsurilor tehnice adecvate pentru integritatea datelor poate fi considerată neglijență. Expunerea publică include alertele de securitate din Gmail/Outlook pentru destinatar și rapoartele de deliverability scăzută.

🔧 SOLUȚIE PROFESIONISTĂ (PAȘI CONCREȚI)

Un profesionist va verifica absența recordului folosind `dig TXT auditope.com` sau `nslookup -type=TXT auditope.com`. Configurația exactă necesară este un record TXT la rădăcina domeniului: `v=spf1 mx -all` (pentru a permite doar serverele MX să trimită emailuri) sau `v=spf1 include:_spf.google.com -all` dacă folosiți Google Workspace. Pașii de implementare includ: 1) Accesați panoul DNS al registrarului; 2) Adăugați un record TXT nou; 3) Introduceți valoarea exactă; 4) Salvați și așteptați propagarea (TTL). Validarea se face rulând din nou `dig TXT auditope.com` și verificând prezența șirului `v=spf1`. Capcana comună este adăugarea mai multor recorduri SPF, ceea ce duce la eroare `permerror`; trebuie să existe un singur record SPF pe domeniu.

💡 TL;DR: *Prevents domain spoofing and phishing attacks, protecting brand reputation.*

CRITIC SECURITATE IMPACT 92/100 ~20 MIN #2

## Implement DKIM Signing for Email Integrity

📋 RECOMANDARE (TL;DR)

Generate a DKIM key pair and publish the public key as a TXT DNS record (e.g., `selector._domainkey.auditope.com`) to cryptographically sign outgoing emails.

⚠ RISC BUSINESS & IMPACT

Fără DKIM, emailurile nu sunt semnate criptografic, ceea ce duce la marcare ca spam sau respingere de către Gmail/Outlook. Acest lucru afectează comunicarea cu clienții și partenerii, reducând rata de conversie a newsletterelor și notificărilor. Conform standardelor industry (RFC 6376), lipsa semnării este o slăbiciune majoră de încredere.

🔧 SOLUȚIE PROFESIONISTĂ (PAȘI CONCREȚI)

Un expert va genera o cheie privată/publică folosind tool-uri precum `opendkim-genkey` sau panoul de administrare al providerului de email (ex: Google Workspace, SendGrid). Configurația DNS necesită un record TXT la `<selector>._domainkey.auditope.com` cu valoarea `v=DKIM1; k=rsa; p=<public_key>`. Pașii sunt: 1) Generați cheia în panoul de email; 2) Copiați cheia publică; 3) Adăugați recordul TXT în DNS; 4) Configurați serverul de email să semneze mesajele cu cheia privată. Validarea se face cu `dig TXT <selector>._domainkey.auditope.com` și verificarea formatului. Capcana comună este tăierea sau adăugarea de spații în cheia publică, care invalidează semnătura.

💡 TL;DR: *Ensures email deliverability and prevents messages from being marked as spam.*

CRITIC | SECURITATE | IMPACT 90/100 | ~15 MIN

#3

## Deploy DMARC Policy for Domain Protection

📋 RECOMANDARE (TL;DR)

Add a DMARC TXT record `_dmarc.auditope.com` with `v=DMARC1; p=quarantine; rua=mailto:dmarc@auditope.com` to monitor and reject unauthorized email usage.

⚠ RISC BUSINESS & IMPACT

Lipsa DMARC permite atacatorilor să folosească domeniul dvs. pentru phishing fără a fi blocați. DMARC oferă rapoarte care vă arată cine abuzează de domeniul dvs., permițând acțiune rapidă. Fără el, sunteți expus la atacuri de business email compromise (BEC), care pot costa mii de euro prin transferuri frauduloase.

🔧 SOLUȚIE PROFESIONISTĂ (PAȘI CONCREȚI)

Un specialist va configura un record TXT la `_dmarc.auditope.com`. Valoarea inițială recomandată este `v=DMARC1; p=none; rua=mailto:dmarc@auditope.com` pentru monitorizare, apoi trecerea la `p=quarantine` și `p=reject`. Pașii: 1) Creați recordul TXT `_dmarc`; 2) Introduceți politica; 3) Configurați adresa de email pentru rapoarte; 4) Monitorizați rapoartele XML primite. Validarea se face cu `dig TXT _dmarc.auditope.com`. Capcana comună este setarea `p=reject` prea devreme, fără a avea SPF/DKIM funcțional, ceea ce blochează emailurile legitime.

💡 TL;DR: *Provides visibility into email abuse and prevents domain spoofing for phishing.*

RIDICAT SECURITATE IMPACT 88/100 ~60 MIN #4

## Harden CSP to Remove unsafe-inline Scripts

📋 RECOMANDARE (TL;DR)

Remove 'unsafe-inline' from script-src in CSP header and use nonces or hashes to allow necessary inline scripts, mitigating XSS risks.

⚠ RISC BUSINESS & IMPACT

CSP cu `unsafe-inline` permite injectarea de scripturi XSS, care pot fura sesiuni de utilizator, cookie-uri și date sensibile. Un atac XSS reușit poate duce la compromiterea conturilor utilizatorilor și pierderea încrederii în platformă. Conform NIS2 și GDPR, măsurile de securitate insuficiente pot duce la amenzi și responsabilitate legală.

🔧 SOLUȚIE PROFESIONISTĂ (PAȘI CONCREȚI)

Un expert în securitate va analiza headerul CSP curent cu `curl -I https://auditope.com/` și va identifica directivele `unsafe-inline`. Configurația corectă implică generarea de nonces dinamice pe server (ex: în PHP/Node.js) și adăugarea lor în headerul CSP: `Content-Security-Policy: script-src 'self' 'nonce-<random_value>';`. Pașii: 1) Identificați scripturile inline necesare; 2) Implementați generarea de nonce la fiecare cerere; 3) Adăugați nonce-ul în tag-ul `<script>` și în headerul CSP; 4) Testați funcționalitatea. Validarea se face verificând că `unsafe-inline` nu mai apare și că scripturile funcționează. Capcana comună este utilizarea nonce-urilor statice, care sunt vulnerabile la atacuri MITM.

💡 TL;DR: *Prevents XSS attacks that can steal user data and sessions.*

RIDICAT GEO/AEO IMPACT 85/100 ~15 MIN #5

## Unblock AI Bots for Citation Visibility

📋 RECOMANDARE (TL;DR)

Update robots.txt to Allow GPTBot, ClaudeBot, and other AI crawlers to access content for citation in generative search results.

⚠ RISC BUSINESS & IMPACT

Blocarea AI bots înseamnă că conținutul dvs. nu va fi citat în rezultatele ChatGPT, Claude sau Perplexity, pierzând o sursă majoră de trafic și autoritate. Competitorii care permit citarea vor domina noile motoare de căutare. Acest lucru afectează vizibilitatea pe termen lung și rata de click-uri organice.

🔧 SOLUȚIE PROFESIONISTĂ (PAȘI CONCREȚI)

Un specialist SEO va accesa `https://auditope.com/robots.txt` și va verifica directivele `Disallow` pentru user-agent-urile AI. Configurația corectă este: `User-agent: GPTBot Allow: / User-agent: ClaudeBot Allow: / User-agent: Google-Extended Allow: /`. Pașii: 1) Editați fișierul robots.txt; 2) Adăugați directivele Allow pentru fiecare bot; 3) Salvați și testați cu Google Search Console Robots Testing Tool. Validarea se face verificând că bot-ii pot accesa paginile cheie. Capcana comună este blocarea accidentală a Googlebot-ului standard prin reguli prea generice.

💡 TL;DR: *Ensures content is cited in AI search results, driving organic traffic.*

RIDICAT PERFORMANȚĂ IMPACT 82/100 ~45 MIN #6

## Optimize Largest Contentful Paint on Mobile

📋 RECOMANDARE (TL;DR)

Optimize hero images, implement lazy loading for below-fold content, and preload critical assets to reduce LCP below 2.5s.

⚠ RISC BUSINESS & IMPACT

Un LCP mare pe mobil crește rata de abandon, deoarece utilizatorii nu așteaptă mai mult de 2.5 secunde. Acest lucru reduce direct conversiile și crește costul de achiziție a clienților. Google folosește Core Web Vitals ca factor de ranking, deci performanța slabă afectează și vizibilitatea organică.

🔧 SOLUȚIE PROFESIONISTĂ (PAȘI CONCREȚI)

Un inginer de performanță va rula Lighthouse pe mobil și va identifica elementul LCP (de obicei o imagine hero). Configurația optimă include: 1) Conversia imaginii în WebP/AVIF; 2) Adăugarea `<link rel='preload' as='image' href='hero.jpg'>` în `<head>`; 3) Redimensionarea imaginii la dimensiunea de afișare. Pașii: 1) Analizați dimensiunea imaginii; 2) Optimizați-o cu tool-uri precum ImageOptim; 3) Adăugați preload; 4) Testați din nou. Validarea se face cu `lighthouse --output=json` și verificarea scorului LCP. Capcana comună este preîncărcarea tuturor imaginilor, ceea ce crește timpul de încărcare inițial.

💡 TL;DR: *Improves mobile UX and reduces bounce rate, boosting conversions.*

RIDICAT PERFORMANȚĂ IMPACT 80/100 ~60 MIN #7

## Reduce Total Blocking Time on Mobile

📋 RECOMANDARE (TL;DR)

Defer non-critical JavaScript, implement code-splitting, and use web workers for heavy calculations to reduce main thread blocking.

⚠ RISC BUSINESS & IMPACT

Un TBT mare face site-ul să pară lent și nesigur, frustrând utilizatorii și reducând timpul petrecut pe site. Acest lucru afectează engagement-ul și rata de conversie, în special pe dispozitivele mobile cu resurse limitate.

🔧 SOLUȚIE PROFESIONISTĂ (PAȘI CONCREȚI)

Un dezvoltator front-end va analiza bundle-ul JS cu Chrome DevTools Performance tab. Configurația optimă implică: 1) Adăugarea `defer` sau `async` la scripturile non-critice; 2) Utilizarea code-splitting-ului (ex: React.lazy); 3) Mutarea calculelor grele în Web Workers. Pașii: 1) Identificați scripturile care blochează; 2) Refactorizați încărcarea; 3) Testați funcționalitatea. Validarea se face cu Lighthouse și verificarea TBT sub 200ms. Capcana comună este deferizarea scripturilor critice pentru layout, care strică randarea.

💡 TL;DR: *Makes the site feel responsive, improving user engagement.*

RIDICAT | ACCESIBILITATE | IMPACT 78/100 | ~30 MIN

#8

## Fix Color Contrast for Accessibility Compliance

📋 RECOMANDARE (TL;DR)

Increase contrast ratio to at least 4.5:1 for normal text by changing text colors (e.g., from #64748b to #334155) on dark backgrounds.

⚠ RISC BUSINESS & IMPACT

Lipsa contrastului face site-ul inutilizabil pentru utilizatorii cu deficiențe de vedere, încălcând WCAG 2.1 AA și legile de accesibilitate (ex: ADA, EN 301 549). Acest lucru poate duce la procese pentru discriminare și pierderea unei părți semnificative a audienței.

🔧 SOLUȚIE PROFESIONISTĂ (PAȘI CONCREȚI)

Un designer sau dezvoltator va folosi tool-uri precum axe DevTools sau Lighthouse pentru a identifica elementele cu contrast scăzut. Configurația corectă implică schimbarea culorii textului pentru a atinge un ratio de 4.5:1. Pașii: 1) Identificați selectorii CSS problematici (ex: `.text-ink-500`); 2) Calculați noua culoare cu un contrast checker; 3) Actualizați fișierele CSS/Tailwind; 4) Testați vizual și automat. Validarea se face cu Lighthouse Accessibility audit. Capcana comună este schimbarea culorii de fundal în loc de text, care poate afecta designul.

💡 TL;DR: *Ensures compliance with accessibility laws and widens audience reach.*

RIDICAT GEO/AEO IMPACT 75/100 ~45 MIN #9

## Improve AI Answer Block Quality

📋 RECOMANDARE (TL;DR)

Restructure content using definition patterns ('X is...') and include concrete facts to improve extraction by AI engines.

⚠ RISC BUSINESS & IMPACT

Conținutul nestructurat nu este extras de AI engines, ceea ce înseamnă că site-ul nu apare ca sursă de autoritate în rezultatele generative. Acest lucru reduce traficul de referință și vizibilitatea brandului în noile canale de căutare.

🔧 SOLUȚIE PROFESIONISTĂ (PAȘI CONCREȚI)

Un specialist în content SEO va analiza secțiunile de pe site pentru a identifica lipsa structurilor clare. Configurația optimă implică rescrierea paragrafelor pentru a începe cu o definiție clară și a include date concrete (cifre, procente). Pașii: 1) Identificați secțiunile cheie; 2) Rescrieți-le folosind modelul 'Subiect + Verbe + Definiție + Date'; 3) Adăugați schema.org markup dacă este necesar; 4) Testați cu tool-uri de citare AI. Validarea se face verificând dacă AI engines extrag passage-urile corect. Capcana comună este adăugarea de conținut generat AI fără verificare umană, care poate fi inexact.

💡 TL;DR: *Increases visibility in AI search results and drives referral traffic.*

RIDICAT PERFORMANȚĂ IMPACT 72/100 ~40 MIN #10

## Eliminate Forced Reflows in JavaScript

📋 RECOMANDARE (TL;DR)

Refactor JavaScript to batch DOM reads and writes, avoiding queries like offsetWidth after style changes to prevent layout thrashing.

⚠ RISC BUSINESS & IMPACT

Forced reflows cauzează lag și stuttering în animații și interacțiuni, ceea ce face site-ul să pară nesigur și de proastă calitate. Acest lucru afectează experiența utilizatorului și poate duce la abandonul site-ului.

🔧 SOLUȚIE PROFESIONISTĂ (PAȘI CONCREȚI)

Un dezvoltator front-end va analiza codul JS cu Chrome DevTools Performance tab pentru a identifica forțarea reflow-ului. Configurația optimă implică gruparea citirilor DOM (offsetWidth, getBoundingClientRect) înainte de scrieri (classList.add, style changes). Pașii: 1) Identificați funcțiile care cauzează reflow; 2) Refactorizați-le pentru a citi toate dimensiunile mai întâi; 3) Scrieți modificările într-un singur pas; 4) Testați performanța. Validarea se face cu Lighthouse și verificarea absenței forțării reflow-ului. Capcana comună este ignorarea impactului asupra dispozitivelor mobile cu CPU slab.

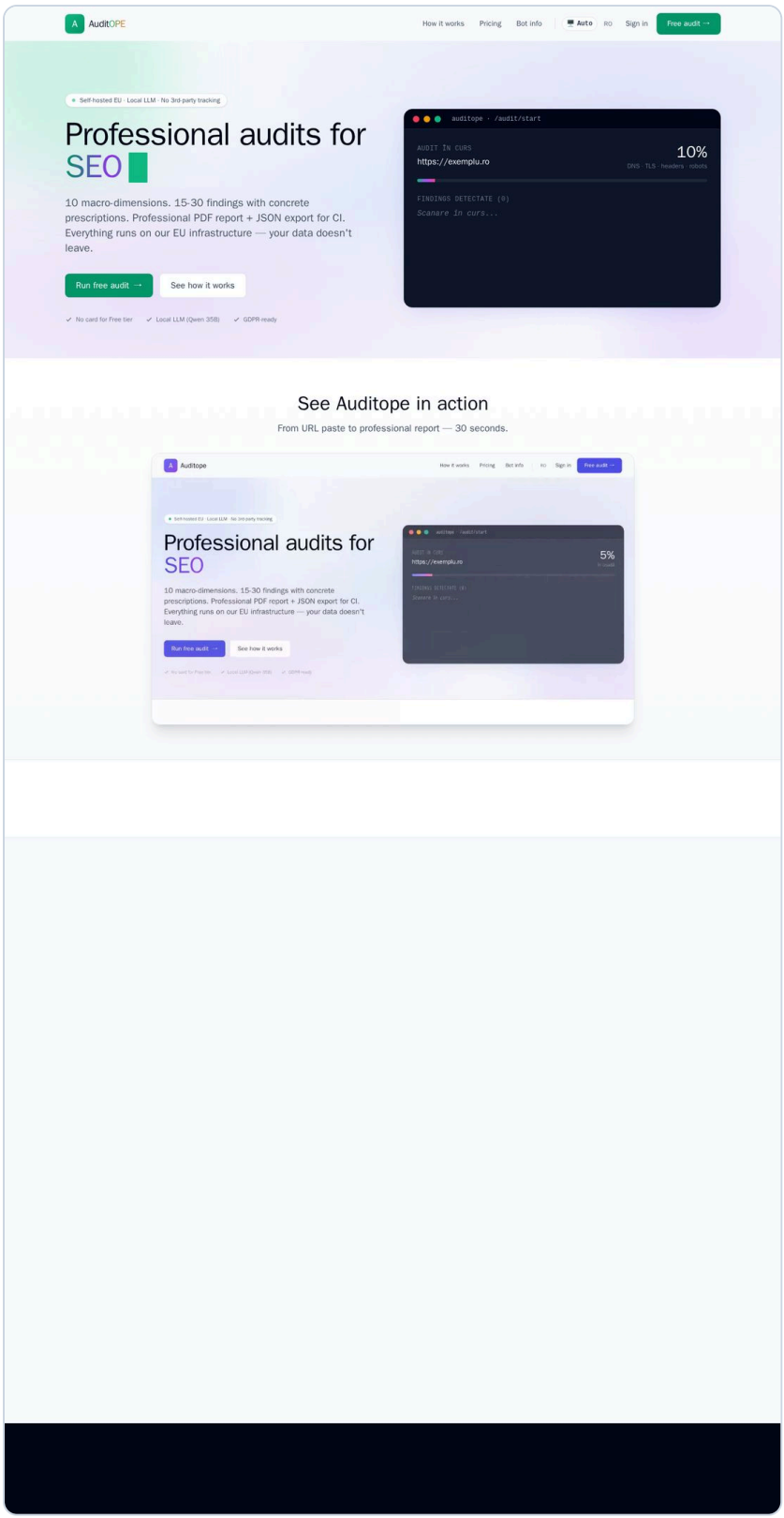
💡 TL;DR: *Improves animation smoothness and overall site responsiveness.*

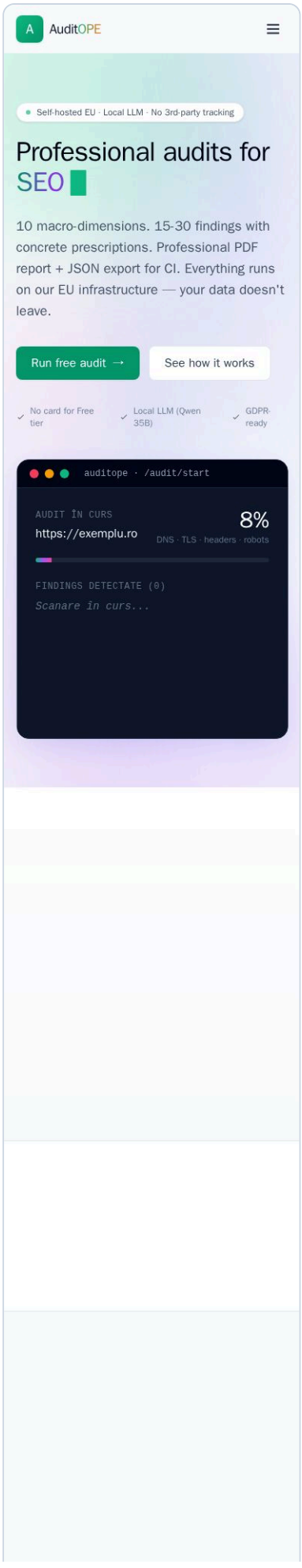
# Referință vizuală

Captură home page la momentul auditului (referință rapidă pentru context).

DESKTOP · VIEWPORT 1440×900 (ABOVE-THE-FOLD + 2 ECRANE)

MOBILE · 390×844




AuditOPE
Self-hosted EU · Local LLM · No 3rd-party tracking
Professional audits for SEO
10 macro-dimensions. 15-30 findings with concrete prescriptions. Professional PDF report + JSON export for CI. Everything runs on our EU infrastructure — your data doesn't leave.
Run free audit →
See how it works
No card for Free tier
Local LLM (Qwen 35B)
GDPR-ready
auditope · /audit/start
AUDIT ÎN CURS
https://exemplu.ro
8%
DNS · TLS · headers · robots
FINDINGS DETECTATE (0)
Scanare în curs...

# Despre acest raport

Acest raport a fost generat automat de **Auditope** printr-un pipeline multi-fazic:

1. Phase 01 — Probes: HTTP/TLS/DNS/security headers/robots.txt/sitemap.xml/llms.txt/.well-known
2. Phase 02 — Lighthouse: audit performance, accessibility, best practices, SEO (mobile + desktop)
3. Phase 03 — Playwright + axe-core: screenshots desktop+mobile, violations WCAG 2.x
4. Phase 04 — GEO/AEO: citability score (llms.txt, JSON-LD, AI bot access, meta SEO, content)
5. Phase 08 — Synthesis LLM: Qwen 35B cross-domain reasoning, prioritizare, recomandări
6. Phase 09 — PDF: raport final cu charts + screenshots

Infrastructură 100% EU-hosted, fără third-party tracking — datele tale nu părăsesc UE.

## CONTACT

Pentru întrebări tehnice sau suport detaliat: technic@auditope.com

*Disclaimer: Acesta este un raport indicativ generat automat. Pentru audit detaliat cu revizuire manuală expert + 90 zile monitorizare + walkthrough call, vezi tier-ul Enterprise pe auditope.com/pricing.*