Auditope

by CAI Technology

Raport Audit

Evaluare automatizată end-to-end

https://belegal.arianextgen.com/

HEALTH SCORE

62

C — necesită îmbunătățiri

auditope.com

Audit ID: f7904210-ac76-4713-9e56-d7485d9a5219

Generat: 23 May 2026 · 11:36 UTC

Sumar executiv

Privire de ansamblu asupra stării site-ului

Site-ul belegal.arianextgen.com prezintă o bază tehnică solidă cu scoruri excelente de accesibilitate și SEO, însă suferă de vulnerabilități critice de conformitate GDPR și lipsa protecțiilor de securitate la nivel de header. Performanța pe mobil este sub așteptări, cu timpi de încărcare mari care afectează experiența utilizatorului și potențialul de conversie. Prioritatea imediată este implementarea banner-ului de consimțământ cookie și activarea headerelor de securitate HSTS și CSP pentru a preveni atacurile de tip MITM și XSS. Optimizarea LCP pe mobil și activarea bfcache sunt pașii tehnici următori pentru îmbunătățirea vitezei.

PUNCTE FORTE

- Scoruri perfecte de accesibilitate (100) pe mobil și desktop.
- Scoruri perfecte de SEO (100) pe mobil și desktop.
- Scoruri perfecte de Best Practices (100) pe mobil și desktop.
- Performanță excelentă pe desktop (97/100).

DETALII AUDIT

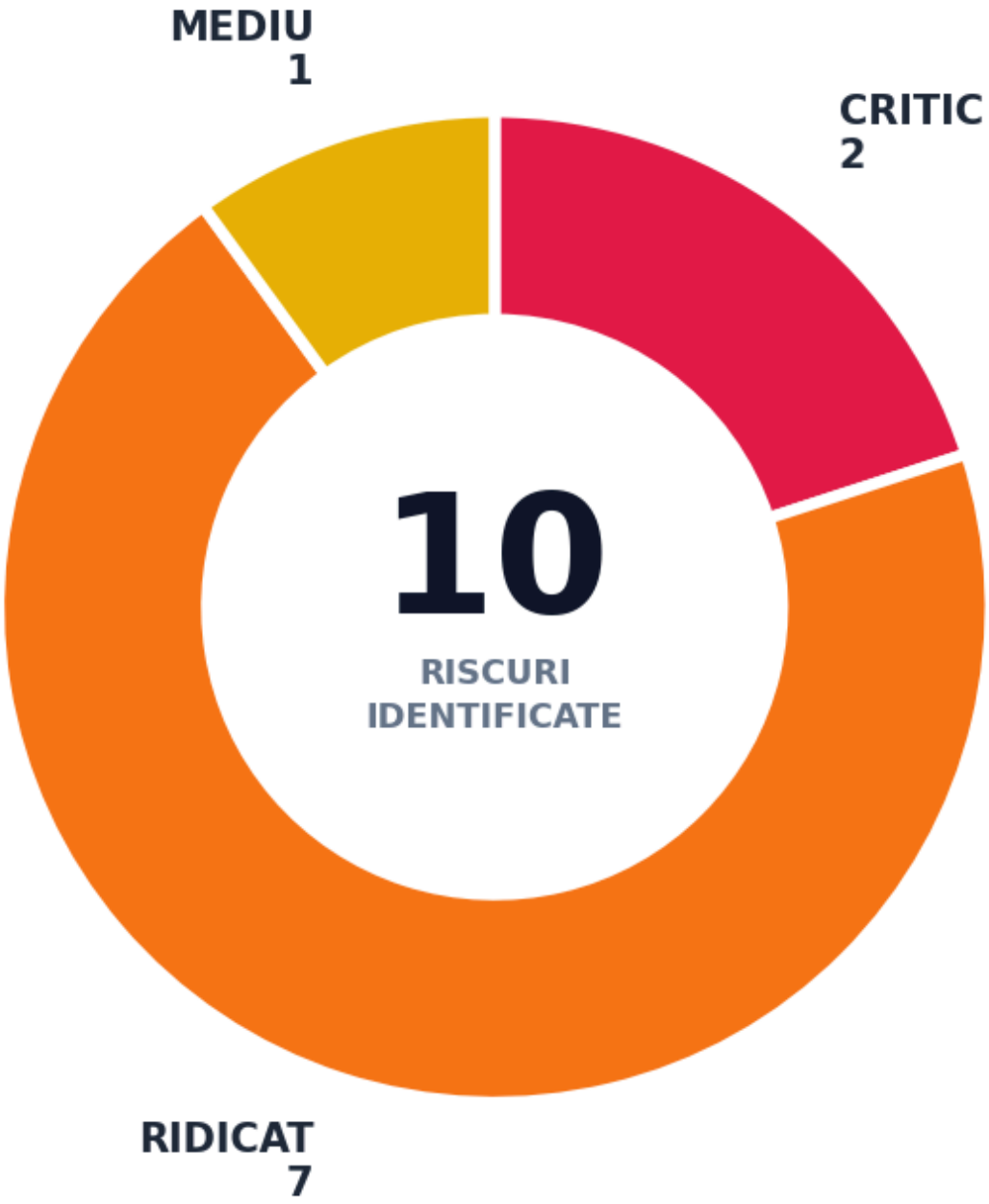
HEALTH SCORE	FINDINGS TOTALE	ACȚIUNI PRIORITARE
62/100	10	10

DISTRIBUȚIE PE SEVERITATE

CRITIC	RIDICAT	MEDIU	SCĂZUT	TOTAL
2	7	1	0	10

DISTRIBUȚIE VIZUALĂ RISCURI

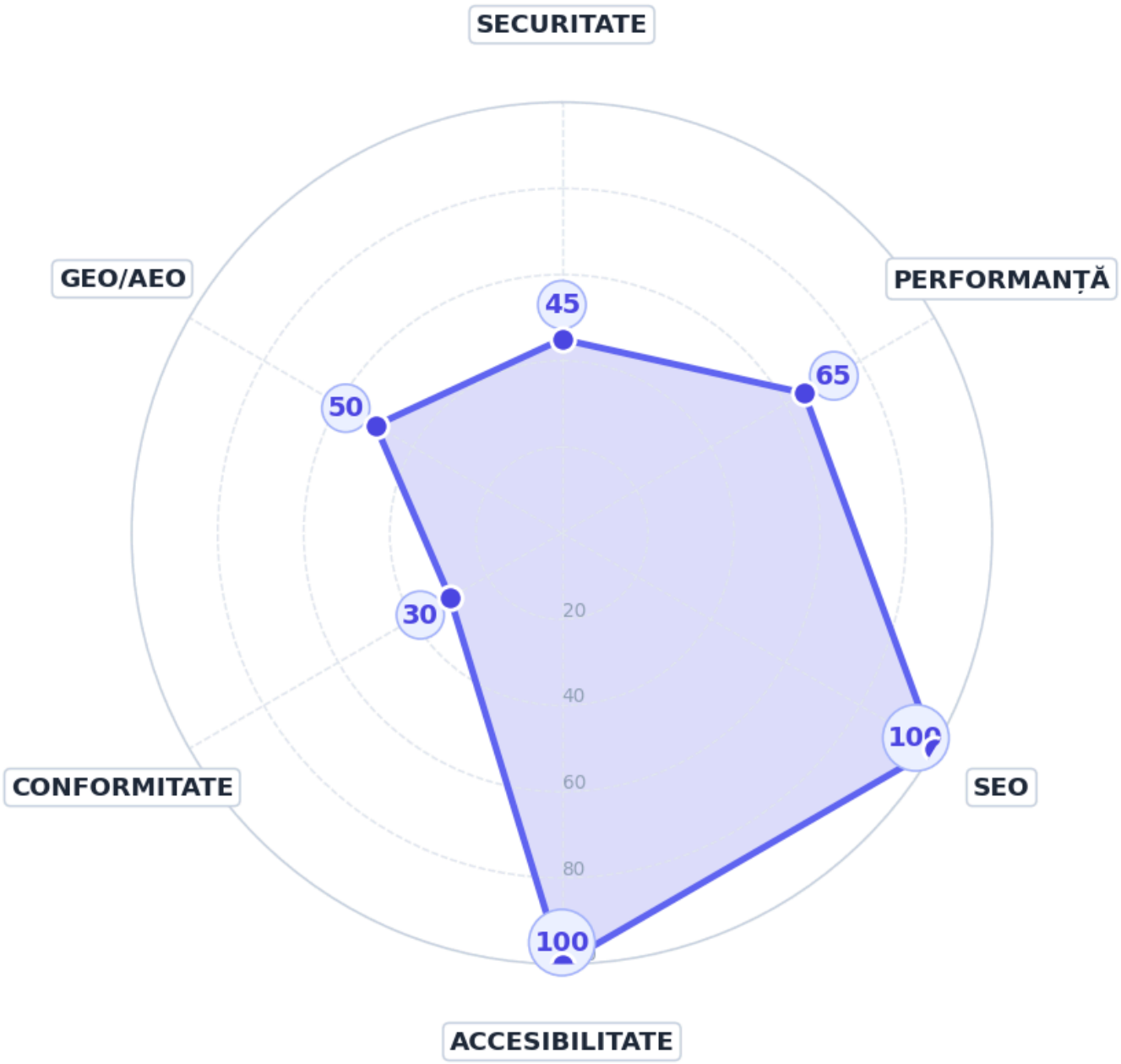
Distribuție riscuri pe severitate



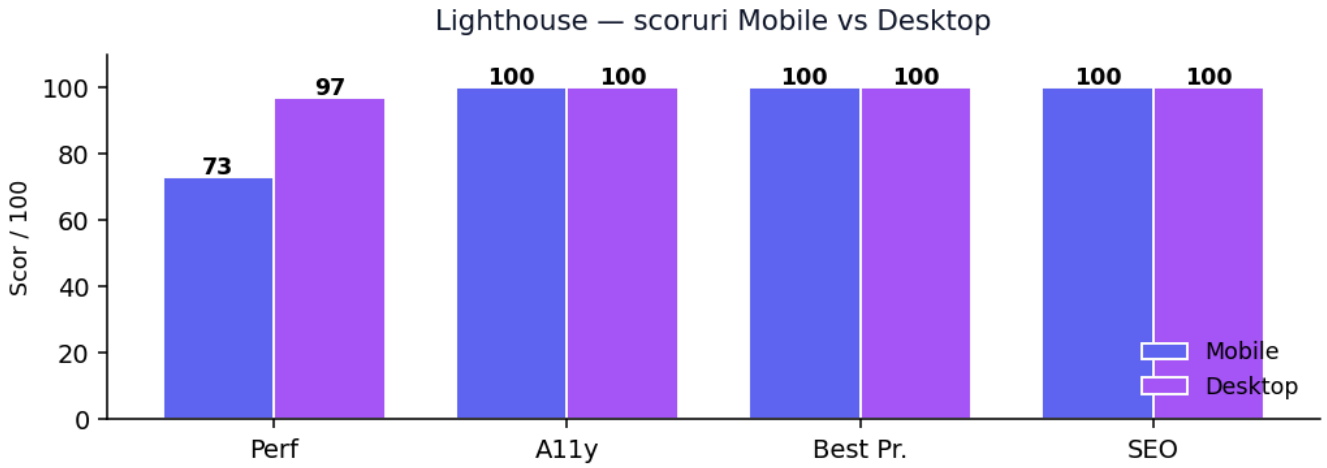
Defalcare scor

Performanța per categorie + comparație Lighthouse mobile vs desktop

RADAR PE CATEGORII



COMPARAȚIE LIGHTHOUSE



SCORURI PER CATEGORIE

Securitate		45/100
Performanță		65/100
SEO		100/100
Accesibilitate		100/100
Conformitate		30/100
GEO/AEO		50/100

Phase 01 — Probes (HTTP/TLS/DNS)

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

STATUS HTTP

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

Redirect hops: 0

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

Body size: 148,312 bytes

CERTIFICAT TLS

Status: Valid

Issuer: Amazon RSA 2048 M01 (Amazon)

Expiră în: 194 zile (`Dec 3 23:59:59 2026 GMT`)

Cipher: `TLS_AES_128_GCM_SHA256`

Versiune: `TLSv1.3`

DNS RECORDS

TYPE	VALUES
A	18.165.171.67, 18.165.171.126, 18.165.171.21, 18.165.171.73
AAAA	2600:9000:2614:4a00:0:12f4:9680:93a1, 2600:9000:2614:7600:0:12f4:9680:93a1, 2600:9000:2614:6800:0:12f4:9680:93a1, 2600:9000:2614:7a00:0:12f4:9680:93a1, 2600:9000:2614:5200:0:12f4:9680:93a1, 2600:9000:2614:9a00:0:12f4:9680:93a1, 2600:9000:2614:8c00:0:12f4:9680:93a1, 2600:9000:2614:8e00:0:12f4:9680:93a1
CNAME	d2pzvgu28umrfe.cloudfront.net.
MX	—
TXT	—
CAA	—

SECURITY HEADERS

HEADER	STATUS
strict-transport-security	✗ lipsă
content-security-policy	✗ lipsă
x-content-type-options	✗ lipsă
x-frame-options	✗ lipsă
referrer-policy	✗ lipsă
permissions-policy	✗ lipsă

FIȘIERE STATICE

FIȘIER	STATUS	MĂRIME
/robots.txt	✓ prezent	84 B
/sitemap.xml	✓ prezent	1,612 B
/llms.txt	✗ 404	52,926 B
/.well-known/security.txt	✗ 404	52,946 B
/.well-known/ai.txt	✗ 404	52,940 B

Phase 02 — Lighthouse

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

SCORURI

CATEGORIE	MOBILE	DESKTOP
Performance	73/100	97/100
Accessibility	100/100	100/100
Best Practices	100/100	100/100
Seo	100/100	100/100

CORE WEB VITALS (MOBILE)

METRIC	VALOARE	SCOR
FCP	1.7 s	92/100
LCP	5.7 s	16/100
TBT	250 ms	84/100
CLS	0	100/100
Speed Index	2.7 s	96/100
TTI	6.0 s	65/100

AUDITS FAILED (TOP 20)

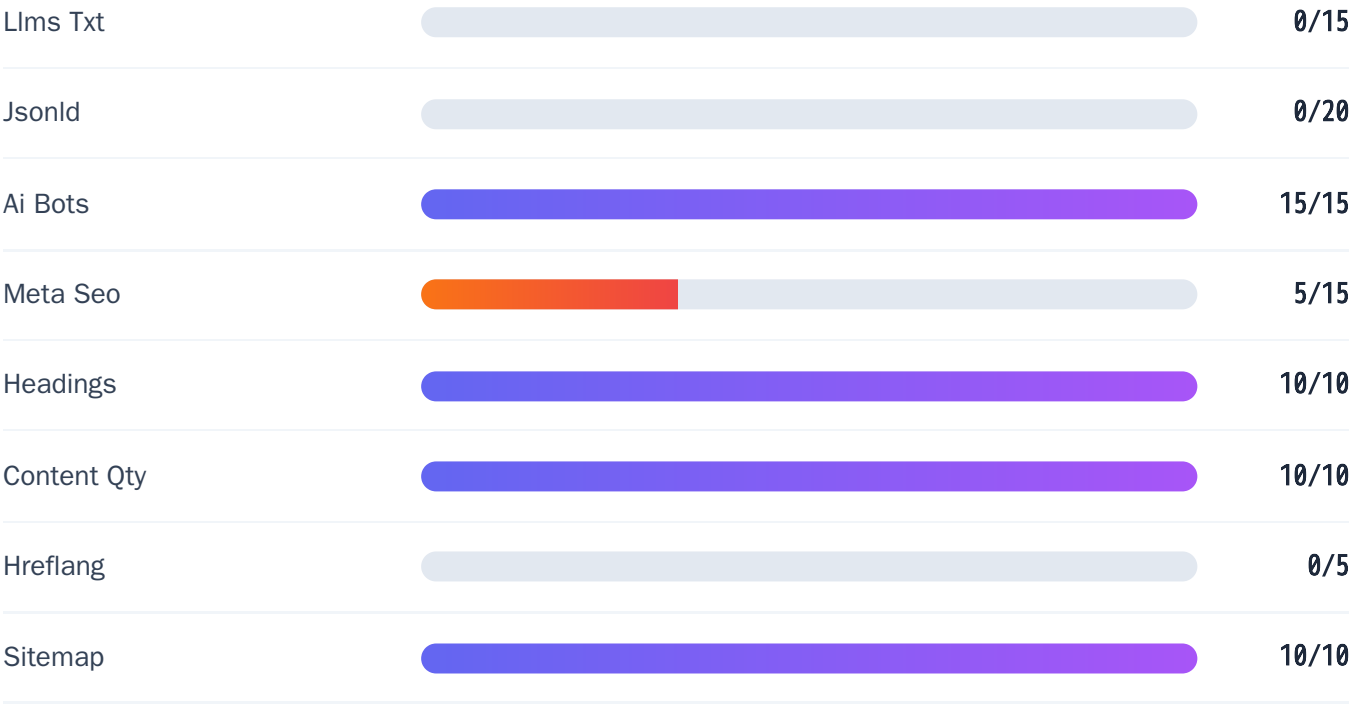
- `largest-contentful-paint`
- `total-blocking-time`
- `max-potential-fid`
- `interactive`
- `label-content-name-mismatch`
- `bf-cache`
- `forced-reflow-insight`
- `lcp-discovery-insight`

Phase 04 — GEO/AEO

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

SCOR CITABILITY: 50/100 — D — POOR

DEFALCARE SEMNALE



Cookies & GDPR compliance

Clasificare via Open Cookie Database (Apache 2.0) — 2 cookies detectate

✓ Cookie banner detectat — consent flow funcțional

Top platforme:

LinkedIn (1)

Tabel cookies detectate

Nume cookie	Categorie	Platformă	Retenție
`__Host-csrfSecret`	Necunoscute	—	
`lang`	Funcționale	LinkedIn	session

Mozilla Observatory · Security headers

Scoring clean room conform methodology Mozilla (zero API extern)

GRADE
F

Mozilla Observatory score

10/100

5 teste trecute · 5 eșuate

Breakdown per test

Csp	-25	Content-Security-Policy header lipsă
Hsts	-20	HSTS header lipsă pe HTTPS
X Frame Options	-20	X-Frame-Options + CSP frame-ancestors absente
Cookies	-20	Cookies fără Secure flag (1)
X Content Type	-5	X-Content-Type-Options absent sau invalid
Referrer Policy	0	Referrer-Policy default/missing
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	0	Permissions-Policy absent (modern best practice)

Standards & Compliance Mapping

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

Standards touched: 9 · 107 findings total cu mapping

Standard / Regulation	Findings (rule_ids)	Count
GDPR Art. 32	`headers-cookies-insecure`	1
Google PWA Checklist	`pwa-manifest-incomplete`	1
Mozilla Web Security Guidelines	`headers-csp-issue` `headers-grade-low`	2
OWASP Top 10 A02:2021	`missing-hsts` `headers-hsts-issue` `cookies-insecure` `headers-cookies-insecure`	4
OWASP Top 10 A05:2021	`missing-csp` `headers-csp-issue` `headers-frame-options-missing` `missing-x-content-type-options` `missing-x-frame-options`	5
RFC 6797	`missing-hsts` `headers-hsts-issue`	2
W3C Service Worker w3.org/TR/service-workers/	`pwa-no-service-worker`	1
W3C Web App Manifest w3.org/TR/appmanifest/	`pwa-manifest-incomplete`	1
WCAG 2.2 SC 3.1.5 (AAA)	`readability-too-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 | CONFORMITATE | IMPACT 98/100 | ~120 MIN

#1

Implementare banner consimțământ cookie (GDPR)

📋 RECOMANDARE (TL;DR)

Implementați un banner explicit care să blocheze cookie-urile neesențiale până la acceptarea utilizatorului, cu butoane distincte pentru 'Acceptă' și 'Respinge'.

⚠ RISC BUSINESS & IMPACT

Lipsa consimțământului explicit expune compania la amenzi GDPR de până la 4% din cifra de afaceri anuală sau 20 milioane EUR. Atacatorii pot exploata cookie-urile de sesiune pentru hijacking dacă nu sunt marcate corect după consimțământ. Datele utilizatorilor sunt procesate ilegal, ceea ce duce la pierderea încrederii și churn rate crescut. Compliance-ul NIS2 și GDPR Art. 7 este încălcat, iar auditorii externi vor semnala acest lucru ca o neconformitate majoră în auditul de securitate.

🔧 SOLUȚIE PROFESIONISTĂ (PAȘI CONCREȚI)

Un profesionist va identifica lipsa bannerului inspectând sursa HTML pentru elemente cu ID-uri comune precum 'cookie-banner' sau verificând dacă există evenimente de blocare a scripturilor la încărcare. Configurația necesară implică integrarea unui CMP (Consent Management Platform) precum Cookiebot sau OneTrust, sau implementarea custom a unui div cu clasa 'cookie-consent' și un script care setează un cookie de sesiune 'consent_given=true' doar după click. Pașii secvențiali sunt: 1) Adăugarea scriptului CMP în <head>, 2) Configurarea regulelor de filtrare a scripturilor terțe, 3) Testarea fluxului de respingere. Validarea se face cu `curl -I https://belegal.arianextgen.com/` pentru a verifica dacă cookie-urile terțe sunt setate înainte de consimțământ (nu ar trebui). Capcana comună este utilizarea unui banner care nu blochează efectiv scripturile, ci doar le afișează, ceea ce nu este conform cu GDPR Art. 7.

💡 TL;DR: *Conformitate legală obligatorie pentru evitarea amenzilor GDPR majore.*

CRITIC | CONFORMITATE | IMPACT 95/100 | ~60 MIN

#2

Respectarea Art. 7 GDPR (Consimțământ activ)

📋 RECOMANDARE (TL;DR)

Asigurați-vă că consimțământul este liber, specific, informat și neechivoc. Nu folosiți pre-bifare sau dark patterns.

⚠ RISC BUSINESS & IMPACT

Consent-ul invalid face orice prelucrare a datelor ilegală, anulând baza legală a procesării. Acest lucru duce la dreptul utilizatorilor de a cere ștergerea datelor (Right to Erasure) și la plângeri la ANSPDCP. Riscul de reputație este ridicat, iar partenerii de business pot rezilia contractele din cauza neconformității GDPR.

🔧 SOLUȚIE PROFESIONISTĂ (PAȘI CONCREȚI)

Un expert va verifica dacă există checkbox-uri pre-bifate în formulare sau dacă butonul 'Acceptă' este singura opțiune vizual prominentă (dark pattern). Configurația corectă necesită interfețe separate pentru 'Necesar' și 'Opțional', cu butoane de dimensiuni egale. Pașii sunt: 1) Auditarea UI-ului pentru dark patterns, 2) Refacerea fluxului de consimțământ cu opțiuni clare, 3) Implementarea logării consimțământului (timestamp, IP, versiune policy). Validarea se face prin testare manuală a fluxului de utilizator și verificarea în baza de date a înregistrărilor de consimțământ. Capcana este confuzia între 'termeni și condiții' și 'consimțământul pentru marketing', care trebuie separate.

💡 TL;DR: *Baza legală a prelucrării datelor este invalidă fără consimțământ activ.*

RIDICAT SECURITATE IMPACT 90/100 ~15 MIN #3

Activare HSTS pentru protecție MITM

📋 RECOMANDARE (TL;DR)

Configurați header HSTS cu max-age=31536000, includeSubDomains, preload pentru a preveni downgrade-ul la HTTP.

⚠ RISC BUSINESS & IMPACT

Fără HSTS, atacatorii pot intercepta traficul prin MITM (Man-in-the-Middle) și fura cookie-urile de sesiune sau datele de login. Acest lucru duce la compromiterea conturilor utilizatorilor și pierderea încrederii. Conformitatea PCI-DSS și GDPR necesită protecția datelor în tranzit, iar lipsa HSTS este o neconformitate tehnică majoră.

🔧 SOLUȚIE PROFESIONISTĂ (PAȘI CONCREȚI)

Un DevOps va verifica absența headerului cu `curl -I https://belegal.arianextgen.com/` căutând după 'strict-transport-security'. Configurația necesară este adăugarea `Header always set Strict-Transport-Security "max-age=31536000; includeSubDomains; preload"` în configurația Nginx/Apache sau în Next.js middleware. Pașii sunt: 1) Actualizarea configurației serverului, 2) Repornirea serviciului web, 3) Verificarea răspunsului HTTPS. Validarea se face cu `curl -I http://belegal.arianextgen.com/` (ar trebui să redirecționeze la HTTPS) și `curl -I https://belegal.arianextgen.com/` (trebuie să conțină HSTS). Capcana este setarea max-age prea scurt sau uitarea includeSubDomains, lăsând subdomeniile vulnerabile.

💡 TL;DR: *Previne interceptarea traficului și furtul de date sensibile.*

RIDICAT SECURITATE IMPACT 88/100 ~45 MIN #4

Implementare Content Security Policy (CSP)

📋 RECOMANDARE (TL;DR)

Definiți CSP cu default-src 'self' pentru a bloca executarea scripturilor malițioase (XSS).

⚠ RISC BUSINESS & IMPACT

Fără CSP, site-ul este vulnerabil la XSS (Cross-Site Scripting), unde atacatorii injectează scripturi malițioase. Acest lucru duce la furtul de date, defacement și compromiterea reputației. Conformitatea OWASP Top 10 necesită CSP, iar lipsa lui crește riscul de atacuri automate.

🔧 SOLUȚIE PROFESIONISTĂ (PAȘI CONCREȚI)

Un specialist securitate va genera o politică CSP inițială în modul 'report-only' folosind instrumente precum CSP Evaluator. Configurația va fi `Content-Security-Policy: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsafe-eval'; style-src 'self' 'unsafe-inline';` (ajustat după audit). Pașii sunt: 1) Adăugarea headerului în modul report-only, 2) Monitorizarea rapoartelor de încălcare, 3) Trecerea la modul strict. Validarea se face cu `curl -I` și verificarea consolei browserului pentru erori CSP. Capcana este blocarea funcționalității legitime (ex: Google Fonts, Analytics) din cauza regulelor prea stricte.

💡 TL;DR: *Protejează împotriva atacurilor XSS și injectării de cod malițios.*

RIDICAT PERFORMANȚĂ IMPACT 85/100 ~60 MIN #5

Optimizare LCP Mobile (5.7s -> <2.5s)

📋 RECOMANDARE (TL;DR)

Optimizați imaginea LCP, folosiți preload pentru resursele critice și reduceți dimensiunea fișierelor.

⚠ RISC BUSINESS & IMPACT

LCP mare pe mobil duce la abandonarea site-ului de către utilizatori (bounce rate crescut) și pierderea conversiilor. Google Core Web Vitals afectează ranking-ul SEO, reducând traficul organic. Fiecare secundă de întârziere poate reduce conversiile cu 7%.

🔧 SOLUȚIE PROFESIONISTĂ (PAȘI CONCREȚI)

Un inginer performance va analiza Lighthouse report pentru a identifica imaginea LCP (probabil hero image). Configurația necesară este adăugarea `<link rel='preload' as='image' href='/path/to/lcp.jpg'>` în <head> și conversia imaginii la WebP/AVIF. Pașii sunt: 1) Identificarea resursei LCP, 2) Optimizarea imaginii, 3) Adăugarea preload, 4) Testare Lighthouse. Validarea se face cu `lighthouse --output=json` și verificarea valorii LCP. Capcana este lazy-loading-ul imaginii LCP, care întârzie încărcarea.

💡 TL;DR: *Îmbunătățește UX-ul mobil și ranking-ul SEO.*

RIDICAT PERFORMANȚĂ IMPACT 80/100 ~30 MIN #6

Activare bfcache pentru navigare rapidă

📋 RECOMANDARE (TL;DR)

Remediați cauzele care previn bfcache: eliminați `Cache-Control: no-store` și scripturi care previn cache-ul.

⚠ RISC BUSINESS & IMPACT

Lipsa bfcache face navigarea lentă, frustrând utilizatorii și crescând rata de abandon. Acest lucru afectează negativ experiența generală și percepția brandului. Performanța scăzută poate duce la pierderea utilizatorilor în favoarea competitorilor mai rapizi.

🔧 SOLUȚIE PROFESIONISTĂ (PAȘI CONCREȚI)

Un developer va inspecta Lighthouse report pentru motivele eșecului bfcache (ex: `CacheControlNoStoreCookieModified`). Configurația necesară este eliminarea headerului `Cache-Control: no-store` de pe paginile statice și asigurarea că scripturile nu modifică cookie-urile după navigare. Pașii sunt: 1) Identificarea scripturilor problematic, 2) Eliminarea headerelor no-store, 3) Testare navigare înapoi/înainte. Validarea se face cu Lighthouse și verificarea dacă pagina se încarcă instantaneu la navigare înapoi. Capcana este utilizarea unor librării care setează cookie-uri la fiecare navigare.

💡 TL;DR: *Îmbunătățește viteza de navigare și experiența utilizatorului.*

RIDICAT PERFORMANȚĂ IMPACT 75/100 ~45 MIN #7

Eliminare Forced Reflow în JavaScript

📋 RECOMANDARE (TL;DR)

Evitați citirea proprietăților geometrice (offsetWidth) după modificarea DOM pentru a preveni reflow-urile forțate.

⚠ RISC BUSINESS & IMPACT

Forced reflow-uri cauzează lag și stuttering pe dispozitivele mobile, afectând negativ experiența utilizatorului. Acest lucru poate duce la frustrare și abandonarea site-ului. Performanța scăzută a interfeței poate afecta percepția profesionalismului brandului.

🔧 SOLUȚIE PROFESIONISTĂ (PAȘI CONCREȚI)

Un developer va identifica codul care cauzează forced reflow în Lighthouse report (sursa neatribuită). Configurația necesară este restructurarea codului JS pentru a citi proprietățile geometrice înainte de a modifica DOM-ul sau folosirea `requestAnimationFrame`. Pașii sunt: 1) Identificarea liniei de cod problematic, 2) Refactorizarea pentru a separa citirea și scrierea, 3) Testare performanță. Validarea se face cu Lighthouse și verificarea absenței alertelor forced reflow. Capcana este utilizarea unor framework-uri care fac reflow-uri automate fără control.

💡 TL;DR: *Elimină lag-ul și îmbunătățește fluiditatea interfeței.*

RIDICAT PERFORMANȚĂ IMPACT 78/100 ~15 MIN #8

Preload imagine LCP în HTML

📋 RECOMANDARE (TL;DR)

Adăugați `fetchpriority='high'` și `<link rel='preload'>` pentru imaginea LCP pentru descoperire imediată.

⚠ RISC BUSINESS & IMPACT

Descoperirea întârziată a imaginii LCP crește timpul de încărcare perceput, afectând UX-ul. Utilizatorii pot părăsi site-ul înainte ca conținutul principal să fie vizibil. Acest lucru afectează negativ metricile de engagement și conversii.

🔧 SOLUȚIE PROFESIONISTĂ (PAȘI CONCREȚI)

Un developer va verifica sursa HTML pentru imaginea LCP (logo sau hero). Configurația necesară este adăugarea atributului `fetchpriority='high'` la tag-ul <img> și adăugarea `<link rel='preload' as='image' href='...'>` în <head>. Pașii sunt: 1) Identificarea imaginii LCP, 2) Adăugarea atributelor, 3) Testare Lighthouse. Validarea se face cu `curl -I` pentru a verifica headerul Link: rel=preload și cu Lighthouse. Capcana este utilizarea lazy-loading pe imaginea LCP, care anulează beneficiul preload-ului.

💡 TL;DR: *Asigură încărcarea rapidă a conținutului principal.*

RIDICAT PERFORMANȚĂ IMPACT 72/100 ~60 MIN #9

Reducere Total Blocking Time (TBT)

📋 RECOMANDARE (TL;DR)

Code-splitting și defer pentru JavaScript non-critic pentru a reduce blocarea thread-ului principal.

⚠ RISC BUSINESS & IMPACT

TBT mare face site-ul să pară lent și nesigur, afectând interacțiunea utilizatorului. Acest lucru duce la frustrare și abandon. Performanța scăzută a interfeței poate afecta negativ percepția brandului și rata de conversie.

🔧 SOLUȚIE PROFESIONISTĂ (PAȘI CONCREȚI)

Un developer va analiza Lighthouse report pentru TBT (250ms) și va identifica scripturile care blochează thread-ul principal. Configurația necesară este adăugarea atributului `defer` sau `async` la scripturi și code-splitting pentru componentele React. Pașii sunt: 1) Identificarea scripturilor grele, 2) Adăugarea defer/async, 3) Code-splitting, 4) Testare. Validarea se face cu Lighthouse și verificarea TBT < 200ms. Capcana este defer-ul scripturilor care sunt necesare pentru randarea inițială.

💡 TL;DR: *Îmbunătățește responsivitatea site-ului pe mobil.*

MEDIU GEO/AEO IMPACT 70/100 ~30 MIN #10

Îmbunătățire Geo-Citability (Scor 50)

📋 RECOMANDARE (TL;DR)

Adăugați fișierele llms.txt, security.txt și ai.txt pentru a îmbunătăți vizibilitatea către AI și securitate.

⚠ RISC BUSINESS & IMPACT

Lipsa acestor fișiere reduce vizibilitatea site-ului către motoarele de căutare AI și tool-urile de securitate. Acest lucru duce la pierderea oportunităților de trafic și parteneriate. Conformitatea cu standardele emergente de securitate (security.txt) este afectată.

🔧 SOLUȚIE PROFESIONISTĂ (PAȘI CONCREȚI)

Un specialist SEO/Geo va verifica absența fișierelor llms.txt, security.txt și ai.txt cu `curl -I https://belegal.arianextgen.com/llms.txt`. Configurația necesară este crearea acestor fișiere în root-ul site-ului cu conținut relevant (ex: security.txt pentru contact securitate, llms.txt pentru LLM indexing). Pașii sunt: 1) Crearea fișierelor, 2) Testare accesibilitate, 3) Verificare indexare. Validarea se face cu `curl -I` pentru a verifica status 200. Capcana este conținutul gol sau incorect al fișierelor.

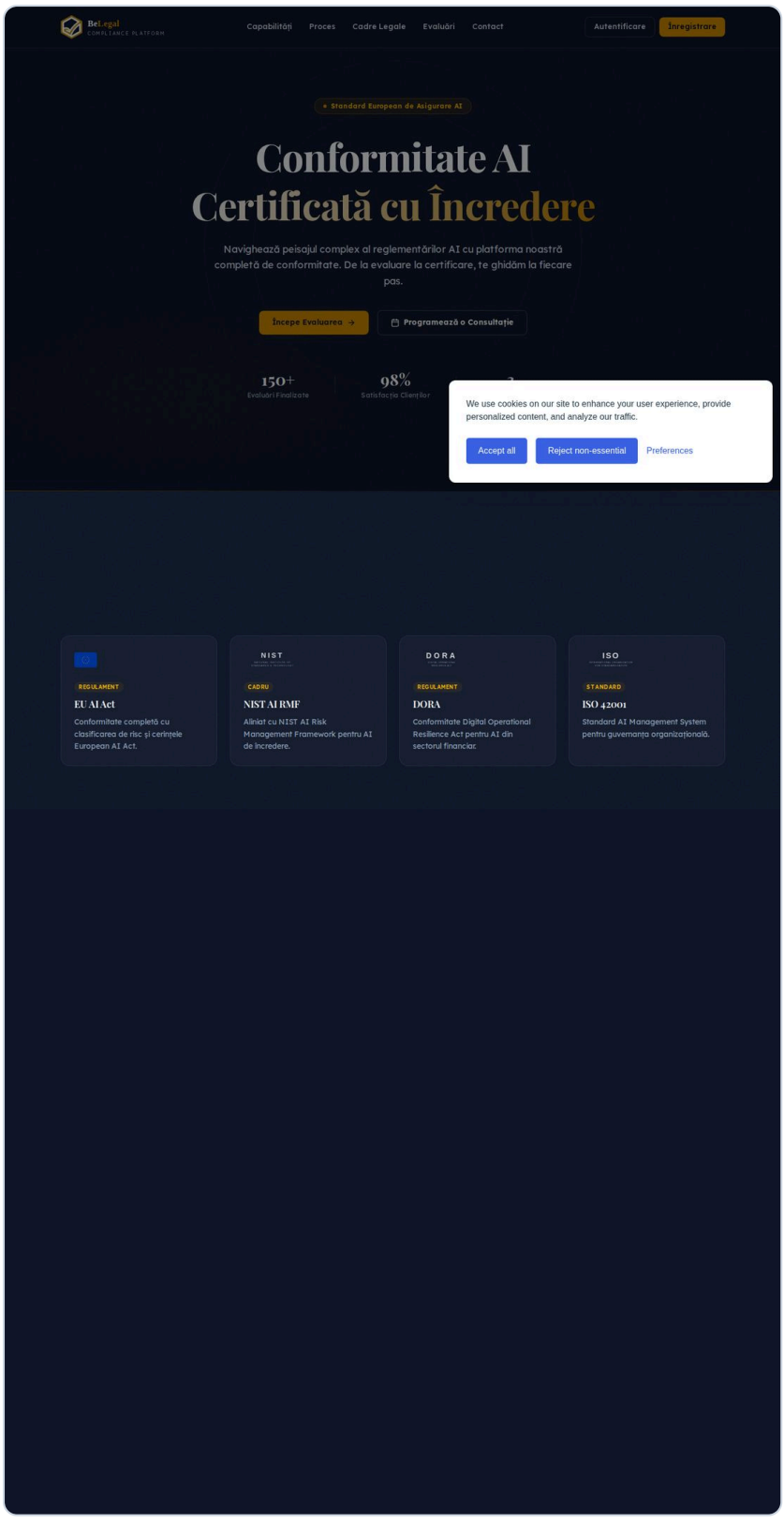
💡 TL;DR: *Îmbunătățește vizibilitatea către AI și tool-urile de securitate.*

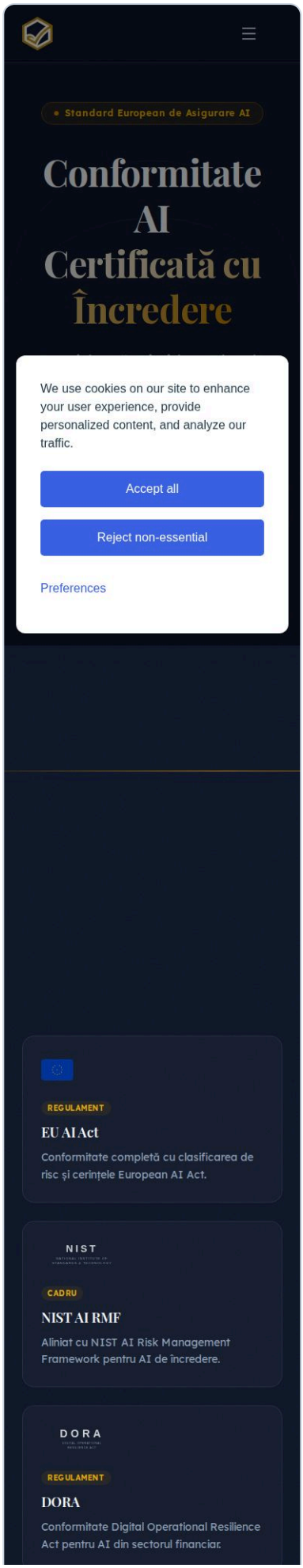
Referință vizuală

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

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

MOBILE · 390×844




Standard European de Asigurare AI
Conformitate AI Certificată cu Încredere
We use cookies on our site to enhance your user experience, provide personalized content, and analyze our traffic.
Accept all
Reject non-essential
Preferences
REGULAMENT
EU AI Act
Conformitate completă cu clasificarea de risc și cerințele European AI Act.
NIST
CADRU
NIST AI RMF
Aliniat cu NIST AI Risk Management Framework pentru AI de încredere.
DORA
REGULAMENT
DORA
Conformitate Digital Operational Resilience Act pentru AI din sectorul financiar.

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.