Audit Report: Odoo Manufacturing ERP Partner in Europe | Avalah — Odoo Gold Partner

Website: https://avalah.ee/
Date: 23.10.2026
Audit Coverage: 100% — all sources returned data
Confidence: high

Pages Audited (1 of 1):

- https://avalah.ee/

Summary of results

Overall Score: 82 / 100
Status: **Needs Improvement**

Performance is genuinely strong — PSI mobile 90 / desktop 99, CLS 0.000, TBT 139 ms, and CrUX field LCP 1060 ms p75 — with the only real drags being mobile FCP 2.56 s, Speed Index 4.24 s, and 196 KB of wasted JavaScript (global.js 122 KB + gtag 74 KB). Accessibility scores 100/100 with 0 axe violations across 41 passes, though 19 color-contrast nodes were left undetermined and the W3C validator found 4 real errors, including an `aria-label` on a `<label>` and an `area-hidden` typo that should be `aria-hidden`. The Security basics verdict is FAILED: HSTS and clickjacking protection are missing at the basic tier, and CSP, Referrer-Policy, Permissions-Policy, COOP and CORP are all absent — this caps the overall below 90. SEO is otherwise clean (canonical, hreflang for en/et/fi, meta description, robots) but the modeled `structuredData` audit fails and the single JSON-LD block reports an unrecognized type. Mobile/desktop divergence is moderate (90 vs 99, FCP 2.56 s vs 744 ms) but not enough to change the verdict; confidence is high because every source returned data.

Per-page scores

 Needs Improvement · https://avalah.ee/

Score	Performance	Accessibility	Best Practices	SEO	Security
82	90	100	100	100	FAILED

PageSpeed Insights — Mobile vs Desktop

*Lower is worse for Performance; higher is worse for LCP and CLS. Worse value is **bolded**.*

Strategy	Performance (M / D)	LCP (M / D)	CLS (M / D)
Mobile vs Desktop	**90** / 99	**2.56 s** / 744 ms	0.000 / **0.000**

Optimization Checklist

2 of 3 passing — 2 pass · 1 warn · 0 fail · 5 n/a

Item	Status	Detail
Page caching plugin / CDN active	**Pass**	Caching plugin detected (WP Rocket) + CDN Cloudflare/Kinsta
Response compressed (gzip / brotli)	**Pass**	Document response is compressed with br.
Images lazy-loaded	N/A	No raster elements found (3 SVGs excluded).
Hero image eagerly loaded	N/A	No raster elements found (3 SVGs excluded).
Hero is a real (not a CSS background-image)	N/A	No CSS background-images detected on raster-image-eligible elements.
Responsive images (srcset /)	N/A	Only 0 raster images on the page (3 SVGs excluded) — responsive-image rule does not apply.
Reasonable number of image sizes	N/A	Too few raster images to evaluate srcset width variety.
JS scripts not blocking in	**Warn**	2 render-blocking scripts in . Move to footer or add defer/async.

Fixes

Priority 1: Critical

Immediate action — impacts user experience, search rankings, or site safety.

1A. Add HSTS and clickjacking protection `Security`

- **Impact:** Transport security, clickjacking, HSTS preload eligibility
- **Problem:** Security basics FAILED: Strict-Transport-Security is missing and neither X-Frame-Options nor CSP frame-ancestors is set, so the page can be framed.
- **Solution:** Send from the origin (or Cloudflare Transform Rules):

  ```
  Strict-Transport-Security: max-age=31536000; includeSubDomains;
  preload
  Content-Security-Policy: frame-ancestors 'self'
  X-Frame-Options: SAMEORIGIN
  ```

  Then submit the domain at hstspreload.org once the max-age has been stable for a few weeks.

Priority 2: Important

Essential for compliance, user reach, and search visibility.

2A. Cut unused JavaScript from theme bundle and GTM `Performance`

- **Impact:** TBT, FCP, Speed Index, mobile Performance score
- **Problem:** Lighthouse reports 122 KB wasted in global.7edaaf903ba7302f.js and 74 KB in gtag.js; gtag also produces 122 ms + 61 ms long tasks and is the single heaviest request at 186.1 KB.
- **Solution:**
  - Audit `global.js` for dead modules (jQuery plugins, unused sliders) and split per-template bundles so the homepage ships only what it uses.
  - Load GTM/gtag after first interaction or on `requestIdleCallback`, and keep consent-mode gating so the tag does not fire before CookieYes resolves.
  - Drop `jquery-migrate.min.js` if no legacy plugin depends on it.

2B. Remove the 2 render-blocking scripts in `Performance`

- **Impact:** FCP, LCP, Speed Index
- **Problem:** The optimized-web checklist flags 2 render-blocking scripts in `<head>`: iframemanager.js and the CookieYes client script.
- **Solution:**
  - Add `defer` to `iframemanager.js` (it is only needed once a consent-gated embed is clicked).
  - Load the CookieYes banner script with `defer` or inject it after `DOMContentLoaded`; the banner does not need to block first paint.

- Verify the WP Rocket "Delay JS execution" option covers both.

2C. Improve mobile FCP and Speed Index `Performance`

- **Impact:** FCP (2.56 s), Speed Index (4.24 s), mobile Performance score
- **Problem:** Mobile FCP is 2.56 s and Speed Index 4.24 s versus 744 ms on desktop — a 1.8 s+ gap that dominates the mobile score gap (90 vs 99).
- **Solution:**
  - Inline critical CSS for the above-the-fold hero and defer the 4 external stylesheets (34.6 KB) plus 30.4 KB of inline CSS.
  - Preload the Geologica woff2 (24.4 KB, 149 ms) and self-host it to remove the fonts.googleapis.com → fonts.gstatic.com chain.
  - Address the `network-dependency-tree-insight` failure by flattening the CSS → font → script request chain.

2D. Add Referrer-Policy, Permissions-Policy, COOP and CORP `Security`

- **Impact:** Information leakage, feature abuse, cross-origin isolation
- **Problem:** All four headers are missing per the security headers scan (advanced tier), and 2 of 2 cross-origin scripts lack Subresource Integrity.
- **Solution:**

```
Referrer-Policy: strict-origin-when-cross-origin
Permissions-Policy: camera=(), microphone=(), geolocation=(),
interest-cohort=()
Cross-Origin-Opener-Policy: same-origin
Cross-Origin-Resource-Policy: same-origin
```

  Add `integrity` + `crossorigin` to the two cross-origin `<script>` tags where the vendor publishes hashes.

2E. Fix structured data `SEO`

- **Impact:** Rich results eligibility, structuredData modeled audit
- **Problem:** The modeled `structuredData` audit fails and the single JSON-LD block reports type "Unknown", so no Organization/Service markup is being recognized.
- **Solution:** Replace the block with explicit, valid schema:

```
{"@context":"https://schema.org","@type":"Organization","name":"Ava
lah","url":"https://avalah.ee/","logo":"https://avalah.ee/logo.png"
,"sameAs":["…"]}
```

Add `Service` markup for the Odoo implementation offering and validate at validator.schema.org.

2F. Fix the 4 W3C ARIA/markup errors `Accessibility`

- **Impact:** Screen reader correctness, HTML validity
- **Problem:** W3C reports 4 errors: `area-hidden` (typo for `aria-hidden`) on the header search form, an empty `name` on the theme-toggle checkbox, a `<p>` inside a `<span>` in the footer, and `aria-label` on a `<label>` associated with a labelable element.
- **Solution:**
  - Line 441: `area-hidden="true"` → `aria-hidden="true"`.
  - Line 1048: remove the empty `name=""` from the theme-toggle input.
  - Line 1093: change the footer `<span class="copyright">` to a `<div>` (or the inner `<p>` to a `<span>`).
  - Line 1049: drop `aria-label` from the `<label>`; put the accessible name on the input or use visually-hidden text inside the label.

2G. Block the WordPress installer and harden the login path `Security`

- **Impact:** Account takeover surface
- **Problem:** Security basics flags `/wp-admin/install.php` as reachable and the login form served on the default `/wp-login.php` path.
- **Solution:**

```
<Files "install.php">
  Require all denied
</Files>
```

  - Add rate limiting / CAPTCHA on `/wp-login.php` (Cloudflare WAF rule or a login-protection plugin).
  - Optionally move the login to a custom path and require 2FA for admin accounts.

Priority 3: Best Practice

Recommended for long-term maintainability.

3A. Verify the 19 undetermined color-contrast nodes `Accessibility`

- **Impact:** WCAG 1.4.3 contrast
- **Problem:** axe returned 0 violations but could not determine contrast for 19 nodes (gradients/alpha backgrounds), plus 1 node with an invalid ARIA attribute value.

- **Solution:**
  - Manually sample each flagged node in DevTools against its actual composited background; target ≥4.5:1 for body text and ≥3:1 for large text.
  - Fix the single `aria-valid-attr-value` node flagged as incomplete.

3B. Disambiguate repeated vague link text `SEO`

- **Impact:** Anchor text quality, screen reader link lists
- **Problem:** The page repeats identical anchor text: "book a consultation" ×3, "services" ×2, "solutions" ×2, "references" ×2, "about us" ×2, "contact" ×2.
- **Solution:**
  - Make each anchor self-describing ("Book an Odoo consultation", "Odoo manufacturing services") or add `aria-label` where the visible text must stay short.
  - Ensure the repeated CTAs point to distinct destinations or consolidate them.

3C. Add a nonce-based CSP `Security`

- **Impact:** XSS defense-in-depth
- **Problem:** Content-Security-Policy is missing entirely. Site signals show no auth, payments, or user-generated content, so XSS impact is limited — hence P3 rather than P1.
- **Solution:** Deploy a nonce + `'strict-dynamic'` policy rather than a flat allowlist:

  ```
  Content-Security-Policy: default-src 'self'; script-src 'nonce-{random}' 'strict-dynamic'; object-src 'none'; base-uri 'none'; frame-ancestors 'self'
  ```

  Roll out in Report-Only first — the page loads GTM, CookieYes and Google Fonts, which will need nonces or self-hosting.

3D. Reduce field TTFB and browser revalidation `Performance`

- **Impact:** TTFB (803 ms p75), repeat-visit LCP
- **Problem:** CrUX TTFB p75 is 803 ms ("average") while lab TTFB is 3 ms, and the document is served with `cache-control: public, max-age=0, s-maxage=86400`, forcing browser revalidation on every navigation.
- **Solution:**
  - Raise `max-age` for the HTML to a short but non-zero value (e.g. `max-age=60, s-maxage=86400, stale-while-revalidate=86400`) so repeat visits skip the round trip.

    - Investigate origin latency behind Cloudflare/Kinsta for uncached HTML requests.

3E. Add dimensions to the 3 remaining images `Best Practices`

- **Impact:** CLS safety margin
- **Problem:** HTML inventory reports 3 images without explicit width/height (the CookieYes consent SVGs).
- **Solution:**
    - If the consent banner markup is theme-controlled, add `width` / `height` to the SVG `<img>` tags.
    - If injected by CookieYes, raise it with the vendor or override via CSS with fixed intrinsic sizing.