TLP:CLEAR – Disclosure is not limited

ClosedSources

Independent Third-Party Risk Practice · Dublin, Ireland

SUPPLIER DUE DILIGENCE REPORT

Brenlisk Software Limited (fictional)

Assessment tier: Tier 2 Standard Assessment

SAMPLE REPORT – FICTIONAL SUPPLIER

This document is a published sample illustrating the format and method of a ClosedSources supplier due diligence report. “Brenlisk Software Limited” is a fictional company. Its domain uses the .example namespace, which is reserved by Internet standard (RFC 2606) and cannot be registered, so no real organisation can correspond to it. All data, identifiers, dates and findings are illustrative. The sources cited are real; they are the sources used in live engagements, and each section states the exact check a reader can run against any real supplier.

Report reference	CS-VDD-2026-000 (sample)
Prepared for	Sample Client Ltd (fictional)
Prepared by	ClosedSources
Date of issue	4 August 2026 (illustrative)
Assessment period	21 July – 1 August 2026 (illustrative)
Version	1.0
Methodology version	1.2 – published at closedsources.com
Classification	TLP:CLEAR. This sample may be shared without restriction.

Document control

Handling

This sample is classified TLP:CLEAR under the FIRST Traffic Light Protocol v2.0 and may be shared without restriction. A live client report is issued TLP:AMBER, with distribution limited to the recipient organisation and those with a need to know.

1. Engagement basis and scope

1.1 Purpose

This report records the outcome of independent due diligence performed on Brenlisk Software Limited ("the Supplier") at the request of Sample Client Ltd ("the Client"), to support the Client's assessment of the Supplier prior to a contractual arrangement for the provision of a cloud-hosted document management service.

1.2 Regulatory and standards context

The assessment is structured so that its outputs can be relied upon as due diligence evidence under the following frameworks, to the extent each applies to the Client:

Framework	Relevant provision
Regulation (EU) 2022/2554 (DORA)	Article 28(4): pre-contract assessment and due diligence on ICT third-party service providers; Article 28(3): register of information inputs; Article 29: sub-outsourcing / subcontracting conditions
EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02)	Section 12.2: due diligence on the service provider prior to outsourcing
Central Bank of Ireland Cross-Industry Guidance on Outsourcing (2021)	Part B §3: due diligence expectations for regulated firms
Directive (EU) 2022/2555 (NIS2)	Article 21(2)(d): supply chain security, including security-related aspects of relationships with direct suppliers
ISO/IEC 27001:2022	Annex A controls A.5.19–A.5.23 (supplier relationships) and A.8.21 (security of network services)

1.3 Scope of this tier

The assessment was performed at Tier 2 (Standard Assessment), which includes all Tier 1 checks. Section 6 (Enhanced Due Diligence) is not in scope for this engagement and was not assessed.

1.4 Limitations

Findings are based solely on information available from public and open sources as at the collection dates recorded in the Source register (Section 8). No access to the Supplier's internal systems, personnel or premises was sought or obtained. This report is not an audit, does not constitute a certification of the Supplier, and does not express an opinion on matters outside the recorded scope. Verification of a claim means verification against the public record, not attestation of internal practice.

Sample notice: the Supplier in this document is fictional and every data point is illustrative. In a live report, each entry in the Source register resolves to a live link, an archived copy, and a retrieval date.

2. Executive summary

2.1 Overall assessment

Overall risk rating	Moderate
Findings raised	0 critical / 1 high / 2 medium / 1 low / 1 informational
Identity verified	Yes

The Supplier is a verifiably registered Irish private limited company with a single, clearly identified beneficial owner and no sanctions, PEP or adverse media exposure. Its production infrastructure is consistent with its claimed EU hosting. Three matters warrant attention before reliance. First, the Supplier's domain publishes no DMARC policy, leaving it exposed to exact-domain email spoofing of the kind used in invoice redirection fraud (F-4.1). Second, an ISO/IEC 27001 certification stated on the Supplier's website could not be located in the public certification registers and should be evidenced by certificate number before it is relied upon (F-4.2). Third, a transactional email provider observable in the Supplier's own DNS records does not appear on its published subprocessor list (F-5.1). Each has a straightforward remediation and none prevents onboarding if addressed contractually.

2.2 Rating scale

Rating	Meaning
Critical	Evidence of active compromise, sanctioned parties, or misrepresented identity. Escalate before any reliance on the Supplier.
High	A verified exposure or record materially inconsistent with the Supplier's claimed posture. Remediation or contractual mitigation expected before or promptly after onboarding.
Medium	A weakness or inconsistency warranting monitoring or clarification with the Supplier.
Low	A minor deviation from good practice with limited direct exposure.
Informational	Context relevant to the arrangement; no action implied.

3. Entity verification (Tier 1)

Confirms that the Supplier is who it claims to be. Every attribute is verified against a primary public record; the Source register gives the full citation for each source reference.

Attribute	Finding	Source	Verified
Registered legal name	Brenlisk Software Limited. Matches the name used on the website and in contracts.	S-01	22 Jul 2026
Registration number / registry	CRO no. 0000000 (illustrative), private company limited by shares, incorporated 12 March 2019, status Normal.	S-01	22 Jul 2026
Legal Entity Identifier (LEI)	No LEI issued. Not required for a supplier of this type; noted for the Client's register of information.	S-02	22 Jul 2026
Registered address	Registered office at a serviced-office address in Dublin 2; trading address in Sandyford per the website. Consistent across filings.	S-01	22 Jul 2026
Trading names / domains	Trades as "Brenlisk". Primary domain brenlisk.example, registered 2019 to the company (registrant organisation matches the CRO record).	S-03	23 Jul 2026
Directors and officers	Two directors: Aoife Sample and Liam Specimen (fictional). Consistent across the incorporation filing and the latest annual return.	S-01	22 Jul 2026
Beneficial ownership	Single beneficial owner (Aoife Sample, 100%) per filed documents. No opaque or offshore layer.	S-01, S-04	23 Jul 2026
Sanctions screening (EU consolidated list, OFAC, UK)	No match for the entity, directors or beneficial owner.	S-05	23 Jul 2026
Politically exposed persons	No match.	S-05	23 Jul 2026
Adverse media	No adverse coverage located in targeted news and leak-archive searches.	S-06	24 Jul 2026
Regulatory authorisations claimed vs held	No regulatory authorisation is claimed; none is required for the service provided.	S-01	24 Jul 2026
Public claims vs public record (founding date, headcount, client and partner claims)	Website states "established 2015"; the company was incorporated in 2019. Stated headcount ("25+ specialists") compares to 14 profiles listing the Supplier as employer. See F-3.1.	S-02, S-03	24 Jul 2026

Reproduce this check: *company search at core.cro.ie (Ireland) or the relevant national registry; LEI at search.gleif.org; sanctions and PEP screening at opensanctions.org; domain registration via an ICANN lookup. The same lookups apply unchanged to any real supplier.*

4. Security posture (Tier 2)

Assesses the Supplier's externally observable security posture and the consistency of its public claims. Where a certification is claimed, the claim is checked against the issuing body's public register where one exists. All observation is passive; no scanning beyond public index services, and no access to any Supplier system.

Area	Finding	Source	Verified
Certifications claimed vs verified (ISO 27001, SOC 2)	Website states "ISO 27001 certified". No certificate for the entity was located in IAF CertSearch or in the register of the certification body named on the site. The claim is unverified, not disproved. See F-4.2.	S-07	28 Jul 2026
Breach and incident history	No disclosed breach located; the domain does not appear in breach-notification records searched.	S-08	28 Jul 2026
Credential exposure in public dumps	Nine addresses on the domain appear in historical third-party breach corpora (oldest 2019). Expected background exposure for a company of this age; no current-system indicator.	S-08	28 Jul 2026
Internet-exposed services and infrastructure	Public index services show ports 80/443 only on production hosts. No exposed management interfaces (RDP, SSH, database ports) indexed.	S-09	29 Jul 2026
Email authentication (SPF / DKIM / DMARC)	SPF present (–all) and DKIM signing observed. No DMARC record is published, so receiving servers are given no policy for mail that fails authentication. The domain is therefore exposed to exact-domain spoofing. See F-4.1.	S-10	29 Jul 2026
TLS configuration on primary services	Grade A on the production host; modern protocol versions only; certificate issued by a public CA and rotated on schedule per certificate-transparency history.	S-11	29 Jul 2026
Published security documentation (trust page, VDP)	No security.txt and no vulnerability disclosure policy published. A trust page describes controls in general terms.	S-03	29 Jul 2026

Reproduce this check: *dig TXT _dmarc.<supplier-domain> +short (an empty answer means no DMARC policy); dig TXT <supplier-domain> +short for SPF; certificate checks at iafcertsearch.org; exposure at shodan.io or search.censys.io; TLS at ssllabs.com/ssltest. ClosedSources provides the email authentication portion of this section as a free posture check to any organisation on request.*

5. Subcontracting chain and data locations (Tier 2)

Records the material subprocessors and locations behind the service, supporting the Client's register of information under DORA Article 28(3) and its assessment of sub-outsourcing under Article 29.

Subprocessor	Function	Location(s)	Source
Amazon Web Services	Production hosting	eu-west-1 (Dublin)	S-09, S-12
SendGrid (Twilio)	Transactional email – observed in the Supplier's SPF record; not on the published subprocessor list. See F-5.1.	United States	S-10, S-12
Microsoft Azure OpenAI Service	Document classification feature, per the Supplier's privacy policy	EU region (stated)	S-12

Production is served from AWS eu-west-1, consistent with the Supplier's claim of EU hosting; DNS resolution and certificate-transparency history corroborate this. One staging subdomain visible in certificate-transparency logs resolved to a US region host; there is no indication it processes production data, and it is recorded at F-5.2 for clarification. Transfers outside the EEA arise through SendGrid; the stated mechanism is the EU Standard Contractual Clauses per that provider's data processing terms.

Where the Supplier's published subprocessor list or privacy documentation names hosted AI services (here, Azure OpenAI), each is recorded as an ICT third-party dependency for the Client's register of information, with its stated function and processing location. A supplier's privacy policy and subprocessor page are frequently the only public record of its AI dependencies, and are treated as a primary source for this section.

Reproduce this check: *read the supplier's DPA or subprocessor page directly; compare it against the SPF record (dig TXT <domain> +short), which is a public list of every service authorised to send email as that domain; subdomains at crt.sh; hosting region from the cloud provider's published IP ranges.*

6. Enhanced due diligence (Tier 3)

Not in scope for this engagement. When commissioned at Tier 3, this section records litigation and insolvency searches, regulatory enforcement history, deeper ownership-chain analysis, and financial standing indicators from filed accounts, each with the same source discipline as Sections 3–5.

7. Findings register

Every finding in this report appears here exactly once, with its evidence and its mapping to the frameworks in Section 1.2. Findings are numbered by the section they arise from (F-4.1 is the first finding from Section 4), and each evidence reference carries a short descriptor so a finding remains readable on its own; the full citation for every reference is in Section 8. Nothing is reported that cannot be traced to a recorded source.

ID	Severity	Finding and recommendation	Control mapping	Evidence	Status
F-3.1	Low	The website states “established 2015”; the company was incorporated in March 2019, and stated headcount exceeds the count of publicly listed employees. Predecessor activity as a sole trader may explain the date. Recommendation: clarify with the Supplier; treat length-of-operation and team-size representations in proposals accordingly.	DORA Art. 28(4); EBA GL 12.2	S-02, S-03 (website vs registry record)	Open
F-4.1	High	No DMARC policy is published for the Supplier’s domain. SPF and DKIM alone do not instruct receiving servers to reject mail that fails authentication, so the exact domain can be spoofed in phishing and invoice redirection fraud targeting the Client or the Supplier’s other customers. Recommendation: the Supplier publishes a DMARC record at p=none with aggregate reporting, reviews reports for two to four weeks, then enforces p=quarantine and p=reject.	ISO A.8.21; NIS2 Art. 21(2)(d); DORA Art. 28(4)	S-10 (DNS records of the domain)	Open
F-4.2	Medium	The website states “ISO 27001 certified”, but no certificate for the entity was located in IAF CertSearch or the named certification body’s register. Not all valid certificates are indexed, so the claim is unverified rather than disproved. Recommendation: the Client requests the certificate number, issuing body and scope statement, and verifies directly with the issuer before relying on the claim.	ISO A.5.19–A.5.20; DORA Art. 28(4); EBA GL 12.2	S-07 (IAF register)	Open
F-5.1	Medium	SendGrid is authorised in the Supplier’s SPF record to send email as its domain but does not appear on the published subprocessor list. The list therefore lags the Supplier’s actual dependencies. Recommendation: the Supplier updates its subprocessor list; the Client records SendGrid in its register of information and confirms the transfer mechanism for US processing.	DORA Art. 28(3), Art. 29; NIS2 Art. 21(2)(d)	S-10, S-12 (SPF record; DPA page)	Open
F-5.2	Informational	Production hosting is consistent with the claimed EU data residency. One staging subdomain visible in certificate-transparency history resolved to a US region host, with no indication of production data. Recommendation: address data location for all environments, including non-production, in the contract’s data-location clause.	DORA Art. 28(3); ISO A.5.23	S-09, S-11, S-12 (hosting indexes; crt.sh; privacy policy)	Open

8. Methodology and source register

8.1 Method

In live engagements, all collection and analysis steps are performed by the named analyst against the primary sources cited in the Source register: company and beneficial-ownership registries, sanctions lists, certification-body registers, breach-notification records, DNS and certificate-transparency data, and archived web content. Scripted lookups (for example DNS queries) are run and read by the analyst directly. No generative AI system is used to collect evidence, form findings, or draft the content of findings. Every source is captured with a live link, an archived copy and a retrieval date, and every finding rests on at least two independent public sources or is stated as unverified.

This sample was produced under ClosedSources methodology version 1.2, published at closedsources.com. It illustrates the format of a live report; its data is fictional, and the Source register below names the real sources with illustrative record entries.

8.2 Lawful basis

In live engagements, where personal data of directors, officers or beneficial owners is processed, it is limited to data already lawfully published in official registers and processed under Article 6(1)(f) GDPR (legitimate interests) for the purpose of counterparty due diligence. No special-category data is sought. Data subjects' details are confined to what the cited public record states. This sample contains no real personal data; all names are fictional.

8.3 Source register

Ref	Source	Record / URL	Retrieved
S-01	Companies Registration Office (Ireland)	core.cro.ie – company printout and filed documents (illustrative record)	22 Jul 2026
S-02	GLEIF LEI search; supplier website	search.gleif.org; brenlisk.example/about (illustrative)	22–24 Jul 2026
S-03	Supplier website and domain registration	brenlisk.example; ICANN registration data lookup (illustrative)	23 Jul 2026
S-04	Beneficial ownership record	Filed CRO documents; OpenCorporates (illustrative)	23 Jul 2026
S-05	OpenSanctions	opensanctions.org – entity and person screening (illustrative)	23 Jul 2026
S-06	Targeted news search; OCCRP Aleph	aleph.occrp.org (illustrative)	24 Jul 2026
S-07	IAF CertSearch; certification body register	iafcertsearch.org (illustrative)	28 Jul 2026
S-08	Have I Been Pwned domain search	haveibeenpwned.com (illustrative)	28 Jul 2026
S-09	Shodan; Censys	shodan.io; search.censys.io (illustrative)	29 Jul 2026
S-10	DNS records (SPF, DKIM, DMARC)	dig / mxtoolbox.com against brenlisk.example (illustrative)	29 Jul 2026
S-11	Qualys SSL Labs; crt.sh	ssllabs.com/ssltest; crt.sh certificate-transparency history (illustrative)	29 Jul 2026
S-12	Supplier privacy policy and subprocessor page	brenlisk.example/privacy; /subprocessors (illustrative)	30 Jul 2026

In a live report, every row carries the live URL, an archive link (web.archive.org or archive.today) captured at the moment of viewing, and the retrieval date, so that each finding can be traced to what the source said on the day it was read.

9. Statement of independence

ClosedSources has no commercial relationship with the Supplier, holds no interest in the outcome of the Client's decision, and received no information or payment from the Supplier in connection with any

engagement. The practice operates under the methodology published at closedsources.com; deviations from that methodology, if any, are recorded in Section 8. (This sample assesses a fictional supplier; the statement is shown as it appears in a live report.)

About this sample

This document shows a Tier 2 Standard Assessment. A Tier 1 Screening covers Section 3 only; a Tier 3 Enhanced Due Diligence adds Section 6. Every check shown here uses public sources that any reader can consult, and each section states how to reproduce its checks. The email authentication assessment in Section 4 (SPF, DKIM and DMARC posture, including whether a domain can be spoofed) is available from ClosedSources as a free posture check to any organisation, no engagement required.

ClosedSources · Dublin, Ireland · closedsources.com