VENDOR EXPOSURE

CLIENT EXPOSURE INDEX

Technology vendor exposure assessment

Prepared for Example Client

Date of assessment: **11 November 2026**

Vendors assessed: **2**

Model version: **E-1.0**

Reference: **EB195F93**

Report format: **R-1.3**

Classification: **SAMPLE: the organisation, vendors, people and events in this report are fictional**

> This index represents the customer's individual exposure to the vendor based on the risk dimensions and weighting selected for this assessment. It is not a universal rating of the vendor.

Key findings

The points that matter most in this assessment, taken from the findings that contribute most to your exposure index. Every finding is dated and sourced in the vendor sections and in Appendix A.

Where your exposure is highest

VENDOR	INDEX	HIGHEST AREA	DATA OUTSIDE THE EU/EEA
Kestrel Mobile Security SA	25	Jurisdiction & control 100 (at maximum)	Yes: Singapore (partner), Hong Kong (elevated-risk)
Helvion Vault AG	4	Operational resilience 12	Yes: Switzerland (allied)

The index averages all areas by your weights, so an area at maximum exposure can sit behind a lower index. The highest area is shown for that reason.

Most important findings

- **Kestrel Mobile Security SA** · **Jurisdiction & control** (area exposure 100): Kestrel Mobile Security is wholly owned by Silverreach Technology Holdings Ltd, a company registered in Hong Kong, which acquired the Luxembourg company in November 2022.
- **Kestrel Mobile Security SA** · **Supply chain dependency** (area exposure 39): The vendor's subprocessor list names an analytics provider in Hong Kong that receives device metadata from managed devices, and a cloud provider region in Singapore used for threat-intelligence processing.
- **Kestrel Mobile Security SA** · **Operational resilience** (area exposure 28): Kestrel Mobile Security reports in its recruiting and engineering pages that about 55 percent of its engineers work in its development centre in Shenzhen, with the remaining engineering split between Luxembourg and Poland.

Other vendors: **Helvion Vault AG** (index 4, highest area: Operational resilience 12).

Questions to ask first

- **Kestrel Mobile Security SA:** Obtain the current subprocessor list and add a data-residency clause restricting processing to the EU/EEA.
- **Kestrel Mobile Security SA:** Add an R&D-location disclosure clause given the majority R&D exposure.
- **Helvion Vault AG:** Request the vendor's DR/BCP documentation or ISO 22301 certification status.

SAMPLE REPORT · Fictional data · Reference ID 7E2905F93 · For illustration only; not an assessment of any real vendor

How to read this report

This report shows how exposed **your organisation** is to each technology vendor you selected, based on structural geopolitical, ownership and operational factors documented in public sources. It is **not** a product security audit, not a prediction of incidents, and not a recommendation to keep or replace any supplier. Use it to inform your own risk conversations and contract decisions.

The Client Exposure Index

Each vendor receives an exposure index from 0 to 100 that is calculated for this order only, from the context you described for that vendor and the weights you chose. A higher number means greater exposure for your organisation. The index is not a universal rating of the vendor: another organisation, with another context and other weights, would receive a different number for the same vendor. No verbal category is attached to the index.

> **How to read the number**
>
> 0 means that no documented exposure was found in the areas you selected. 100 means documented exposure at the maximum level in all of the areas you selected. Everything in between is a weighted combination of the areas, using the weights you chose.
>
> Because the number depends on the weights and the context of each order, it is **not comparable** between orders with a different configuration, and a change of weights changes the number without any change in the vendor. To understand a number, read the 'What drives this exposure' box for the vendor.

Your answers and weights

Your answers about how you use a vendor change how much a given type of finding matters for you; they never remove a finding. The weights you set decide how much each of the eight areas counts towards the index. An area with weight 0 is not part of the index, and its section says so.

Legal status flags

A legal status flag (for example a sanctions listing, an official state warning, or a headquarters in a high-risk jurisdiction) is shown above the index. Flags describe official facts, are not weighted, and cannot be switched off.

Charts

Ring	The exposure index for a vendor or for the portfolio, from 0 to 100.
Heatmap	The exposure of each area for each vendor; darker is higher, grey areas are not included.
What makes up the index	The points each area adds to the index; the three largest are named.
Risk areas	Each area's exposure (bar) next to the weight you gave it.
What drives this exposure	The areas contributing most, with your weight and an example finding.
Jurisdiction profile	Where the vendor is headquartered, owned and processes data, on a schematic map.
How your context shaped this	Which finding groups your answers made more or less important (direction only).

Where the information comes from

Every factual statement in this report is backed by independently verifiable records: corporate registries, regulatory and stock-exchange filings, sanctions lists across four regimes, technical vulnerability databases, and the supplier's own formal commitments. Each source is cited, so your auditors can retrace every claim. Where a fact is not documented in any of these, we state so explicitly and assess conservatively — non-disclosure is treated as a risk signal, not as neutral.

Each finding carries its date, the type and domain of its source, and a reference number in square brackets that points to Appendix A. An area without findings has been checked against those sources; where the record is limited, the section says so and the area is assessed conservatively. The data is fixed at the moment the report was generated.

SAMPLE REPORT · fictional data · for illustration only, no assessment of any real organisation · reference EB195F93

Summary

Portfolio at a glance

- **2** vendors assessed for Example Client.
- Position within your portfolio: Highest exposure: Kestrel Mobile Security SA (25 / 100). Lowest exposure: Helvion Vault AG (4 / 100). The spread between them is 21 points.
- No legal status flags were raised for the vendors assessed.
- All eight areas are included in your assessment.

PORTFOLIO EXPOSURE



Average across your vendors, weighted by the importance you assigned.

Exposure by area

	Sanctions exposure	Ownership transparency	Jurisdiction & control	Operational resilience	Cyber hygiene	Supply chain dependency	Financial stability	Regulatory alignment	**Exposure**
Kestrel Mobile Security SA	0	10	100	28	14	39	0	11	**25**
Helvion Vault AG	0	0	10	12	0	0	0	12	**4**

0 25 50 75 100 not included in your assessment

SAMPLE REPORT · fictional data · reference EB195F93
for illustration only; not an assessment of any real organisation

Your vendors

VENDOR	IMPORTANCE	EXPOSURE	HIGHEST AREA
Kestrel Mobile Security SA	High	25	Jurisdiction & control 100 (at maximum)
Helvion Vault AG	High	4	Operational resilience 12

How your context shaped this assessment

Your answers never remove a finding: they change how much a group of findings weighs for your organisation. Findings about sanctions and legal status are never modified by your answers. Only the direction of the effect is shown here.

Kestrel Mobile Security SA

Overall: findings about **data handling and subprocessors, operational dependency and continuity, security posture and regulatory fit** carry more weight.

- Your answer ‘Endpoint technology’ to “What role does this vendor perform in your organisation?” gives more weight on security posture.
- Your answer ‘High’ to “How critical is this vendor to your operations?” gives more weight on operational dependency and continuity.
- Your answer ‘Yes’ to “Does the vendor process, or have access to, sensitive or customer data?” gives more weight on data handling and subprocessors and regulatory fit.
- Your answer ‘Yes’ to “Does the vendor have privileged access to your systems?” gives more weight on data handling and subprocessors and security posture.

Helvion Vault AG

Overall: findings about **data handling and subprocessors, operational dependency and continuity and regulatory fit** carry more weight; findings about **security posture** carry less weight.

- Your answer ‘Cloud & data processing’ to “What role does this vendor perform in your organisation?” gives more weight on data handling and subprocessors, operational dependency and continuity and regulatory fit.
- Your answer ‘High’ to “How critical is this vendor to your operations?” gives more weight on operational dependency and continuity.
- Your answer ‘Yes’ to “Does the vendor process, or have access to, sensitive or customer data?” gives more weight on data handling and subprocessors and regulatory fit.
- Your answer ‘No’ to “Does the vendor have privileged access to your systems?” gives less weight on security posture.

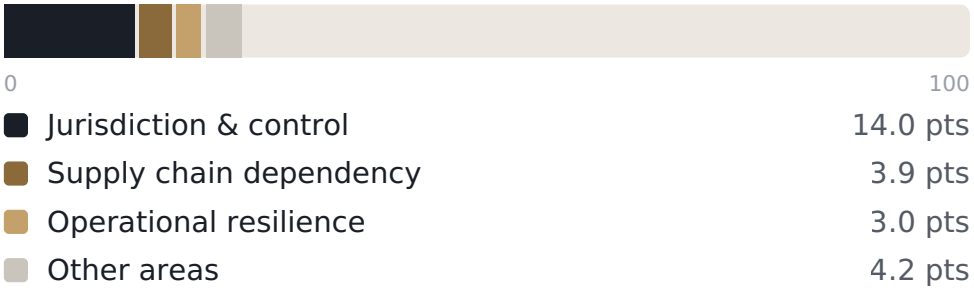
SAMPLE REPORT · Fictional data · Reference only · No real organisation
for illustration only, not an assessment of any real supplier

Kestrel Mobile Security SA

CLIENT EXPOSURE INDEX



WHAT MAKES UP THE INDEX

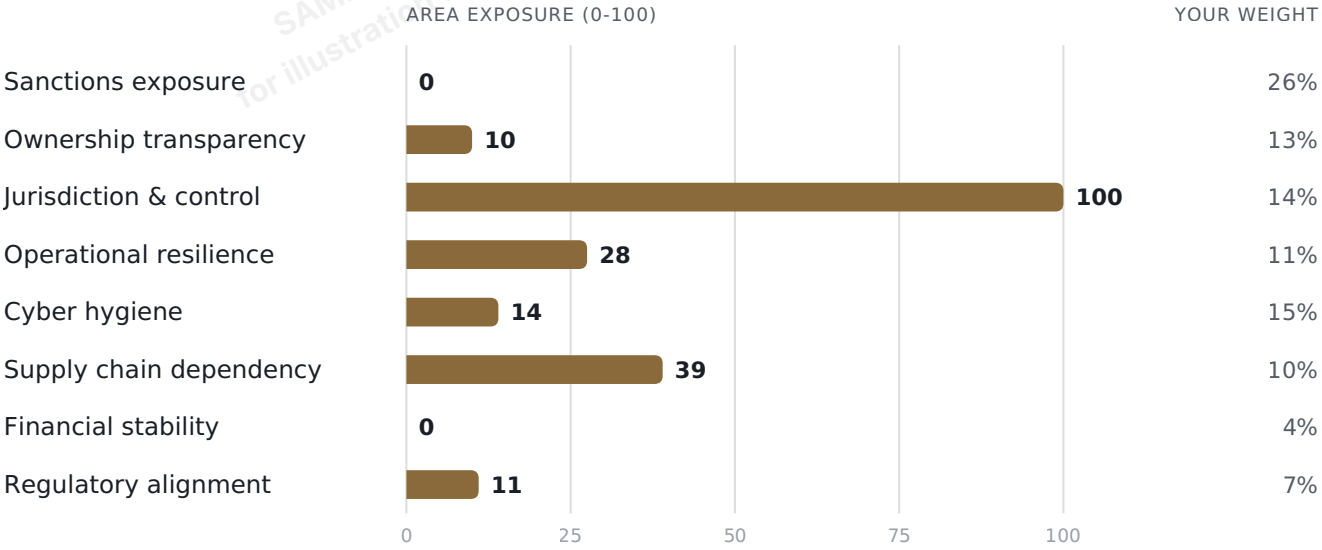


What drives this exposure

Your exposure index for Kestrel Mobile Security SA is driven mainly by Jurisdiction & control, Supply chain dependency and Operational resilience.

- **Jurisdiction & control** (area exposure 100, your weight 14%): for example: “Kestrel Mobile Security is wholly owned by Silverreach Technology Holdings Ltd, a company registered in Hong Kong, which acquired the Luxembourg company in November 2022.”
- **Supply chain dependency** (area exposure 39, your weight 10%): for example: “The vendor's subprocessor list names an analytics provider in Hong Kong that receives device metadata from managed devices, and a cloud provider region in Singapore used for threat-intelligence processing.”
- **Operational resilience** (area exposure 28, your weight 11%): for example: “Kestrel Mobile Security reports in its recruiting and engineering pages that about 55 percent of its engineers work in its development centre in Shenzhen, with the remaining engineering split between Luxembourg and Poland.”

Risk areas



Event timeline

The most significant documented events (up to 10), newest first. Items marked as context do not add to the exposure index.

DATE	EVENT	SOURCE
2026-10-20	A search of the consolidated sanctions lists of the United States, the European Union, the United Kingdom and the United Nations (as of 29 October 2026) returned no match for Kestrel Mobile Security, Silverreach or the named executives. context	Primary record · sanctions-demo.example [1]
2026-09-10	The vendor's subprocessor list names an analytics provider in Hong Kong that receives device metadata from managed devices, and a cloud provider region in Singapore used for threat-intelligence processing. Core customer data is kept in Kestrel's own data centre in Luxembourg.	Vendor statement · trust.kestrel-demo.example [2]
2026-09-10	Kestrel Mobile Security reports in its recruiting and engineering pages that about 55 percent of its engineers work in its development centre in Shenzhen, with the remaining engineering split between Luxembourg and Poland.	Vendor statement · kestrel-demo.example [3, 4]
2026-09-10	No vulnerability-reporting channel (security.txt, a bug-bounty programme or a published disclosure policy) was found for Kestrel Mobile Security; reports are accepted only through the general support address.	Technical · kestrel-demo.example [5]
2026-09-10	The vendor does not publish a data-processing agreement that refers to EU standard contractual clauses for the Hong Kong subprocessor, and offers no support contact in an EU time zone outside Luxembourg business hours.	Vendor statement · trust.kestrel-demo.example [6]
2026-09-10	Kestrel Mobile Security is headquartered in Luxembourg and holds an EU data-protection representative. Its management board consists of three people based in Luxembourg and Warsaw. context	Vendor statement · kestrel-demo.example [7]
2026-04-20	Kestrel Mobile Security holds an ISO/IEC 27001 certificate issued by an accredited body. context	Vendor statement · trust.kestrel-demo.example [8]
2022-11-30	Kestrel Mobile Security is wholly owned by Silverreach Technology Holdings Ltd, a company registered in Hong Kong, which acquired the Luxembourg company in November 2022. The registry documents trace Silverreach to named founders; ownership is fully resolved.	Primary record · rcs-demo.example [9, 10]
2022-11-30	The ownership chain has three levels: Kestrel Mobile Security SA (Luxembourg), Silverreach Technology Holdings (Hong Kong) and a founders' vehicle in the British Virgin Islands.	Primary record · hkregistry-demo.example [11]

Area analysis

Sanctions exposure

Area exposure 0 / 100 · your weight 26%

No matches across four sanctions regimes for the entity, its holding chain, or its executives (as of 2026-11-11).

Documented checks and context for this area

2026-10-20 · Primary record · sanctions-demo.example · Context [1]
A search of the consolidated sanctions lists of the United States, the European Union, the United Kingdom and the United Nations (as of 29 October 2026) returned no match for Kestrel Mobile Security, Silverreach or the named executives.

Items marked as context are documented events that do not add to the exposure index.

Ownership transparency

Area exposure 10 / 100 · your weight 13%

2022-11-30 · Primary record · hkregistry-demo.example [11]
The ownership chain has three levels: Kestrel Mobile Security SA (Luxembourg), Silverreach Technology Holdings (Hong Kong) and a founders' vehicle in the British Virgin Islands.

Jurisdiction & control

Area exposure 100 / 100 · your weight 14%

2026-09-10 · Vendor statement · trust.kestrel-demo.example [2]
The vendor's subprocessor list names an analytics provider in Hong Kong that receives device metadata from managed devices, and a cloud provider region in Singapore used for threat-intelligence processing. Core customer data is kept in Kestrel's own data centre in Luxembourg.

2026-09-10 · Vendor statement · kestrel-demo.example [3, 4]
Kestrel Mobile Security reports in its recruiting and engineering pages that about 55 percent of its engineers work in its development centre in Shenzhen, with the remaining engineering split between Luxembourg and Poland.

2022-11-30 · Primary record · rcs-demo.example [9, 10]
Kestrel Mobile Security is wholly owned by Silverreach Technology Holdings Ltd, a company registered in Hong Kong, which acquired the Luxembourg company in November 2022. The registry documents trace Silverreach to named founders; ownership is fully resolved. The controlling owner is therefore established in a jurisdiction with elevated state-influence risk.

Documented checks and context for this area

2026-09-10 · Vendor statement · kestrel-demo.example · Context [7]
Kestrel Mobile Security is headquartered in Luxembourg and holds an EU data-protection representative. Its management board consists of three people based in Luxembourg and Warsaw.

Items marked as context are documented events that do not add to the exposure index.

Operational resilience

Area exposure 28 / 100 · your weight 11%

2026-09-10 · Vendor statement · kestrel-demo.example [3, 4]
Kestrel Mobile Security reports in its recruiting and engineering pages that about 55 percent of its engineers work in its development centre in Shenzhen, with the remaining engineering split between Luxembourg and Poland.

Cyber hygiene

Area exposure 14 / 100 · your weight 15%

2026-09-10 · Technical · kestrel-demo.example [5]
No vulnerability-reporting channel (security.txt, a bug-bounty programme or a published disclosure policy) was found for Kestrel Mobile Security; reports are accepted only through the general support address.

Supply chain dependency

Area exposure 39 / 100 · your weight 10%

2026-09-10 · Vendor statement · trust.kestrel-demo.example [2]
The vendor's subprocessor list names an analytics provider in Hong Kong that receives device metadata from managed devices, and a cloud provider region in Singapore used for threat-intelligence processing. Core customer data is kept in Kestrel's own data centre in Luxembourg.

Financial stability

Area exposure 0 / 100 · your weight 4%

No financial-stability risk indicators identified for this supplier (as of 2026-11-11).

Regulatory alignment

Area exposure 11 / 100 · your weight 7%

2026-09-10 · Vendor statement · trust.kestrel-demo.example [6]
The vendor does not publish a data-processing agreement that refers to EU standard contractual clauses for the Hong Kong subprocessor, and offers no support contact in an EU time zone outside Luxembourg business hours.

Documented checks and context for this area

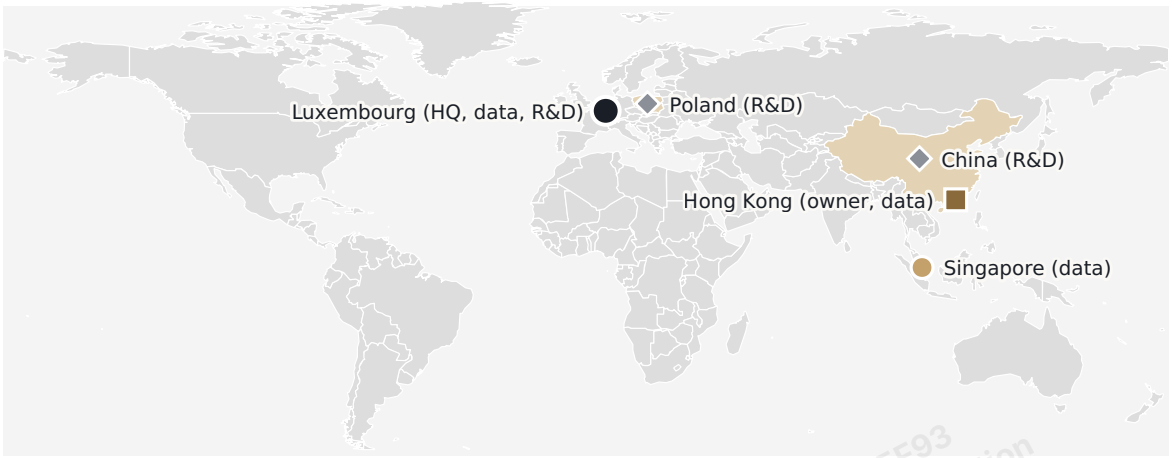
2026-04-20 · Vendor statement · trust.kestrel-demo.example · Context [8]
Kestrel Mobile Security holds an ISO/IEC 27001 certificate issued by an accredited body.

SAMPLE REPORT · fictional data · Reference EB19-FF93
for illustration only; not an assessment of any real organisation

> Items marked as context are documented events that do not add to the exposure index.

Jurisdiction profile

Headquarters: Luxembourg (EU / domestic). Ownership: Ownership structure verified against public records in Hong Kong; no hidden or unresolved ownership layers were identified. R&D concentration: China 55%, Luxembourg 25%, Poland 20%. Data residency: Luxembourg, Singapore, Hong Kong.



SAMPLE REPORT, fictional data, for illustration only; no assessment of any real organisation. Reference ID 195F93

Headquarters	**Luxembourg** · EU / domestic National or EU jurisdiction — full protection of EU law.
Ultimate ownership	**Hong Kong** · Elevated-risk country Ownership structure verified against public records in Hong Kong; no hidden or unresolved ownership layers were identified.
Data and processing locations	• **Luxembourg** · Own data centre · EU / domestic • **Singapore** · Cloud provider, Singapore region · Neutral / partner country • **Hong Kong** · Analytics subprocessor, Hong Kong · Elevated-risk country
R&D footprint	China 55%, Luxembourg 25%, Poland 20%
Can customer data leave the EEA?	Yes: at least one documented processing location is outside the EU/EEA (Singapore, Hong Kong).

What these jurisdictions mean for you

- **EU / domestic**: National or EU jurisdiction — full protection of EU law.
- **Neutral / partner country**: Stable jurisdiction with no specific reservations.
- **Elevated-risk country**: Limited legal predictability or geopolitical tensions relevant to the supply chain.

What could change the assessment

Events that would be reflected in a later assessment of this vendor. They are examples, not a forecast.

Could increase your exposure

- **Sanctions exposure:** A new listing of the vendor, its owners or its directors on a sanctions or export-control list.
- **Cyber hygiene:** A newly disclosed, actively exploited vulnerability or a security incident affecting the vendor's products.
- **Jurisdiction & control:** A change in the legal systems that govern the vendor's headquarters, subsidiaries or data locations.

Could reduce it

- **Jurisdiction & control, Supply chain dependency, Operational resilience:** Independent documentation that the condition behind an existing finding has changed (for example a resolved ownership question or a remediated vulnerability) is taken into account in a later assessment.

Questions worth asking your supplier

- Obtain the current subprocessor list and add a data-residency clause restricting processing to the EU/EEA.
- Add an R&D-location disclosure clause given the majority R&D exposure.
- Request clarification of the UBO's jurisdiction relative to the HQ jurisdiction.
- Request the vendor's business-continuity plan for a single-country operational disruption.
- Request an ownership chart showing all holding-company layers.

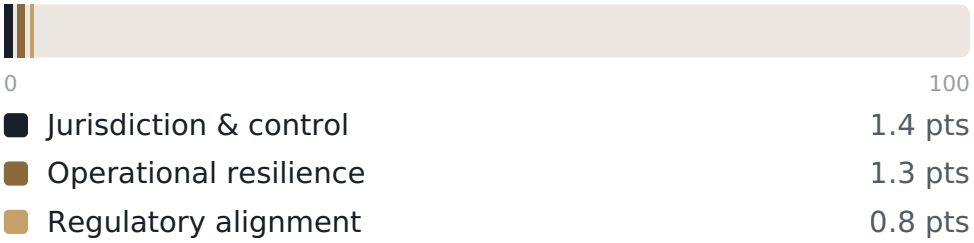
SAMPLE REPORT · fictional data · for illustration only; not an assessment of any real organisation · ref. EB195F93

Helvion Vault AG

CLIENT EXPOSURE INDEX



WHAT MAKES UP THE INDEX



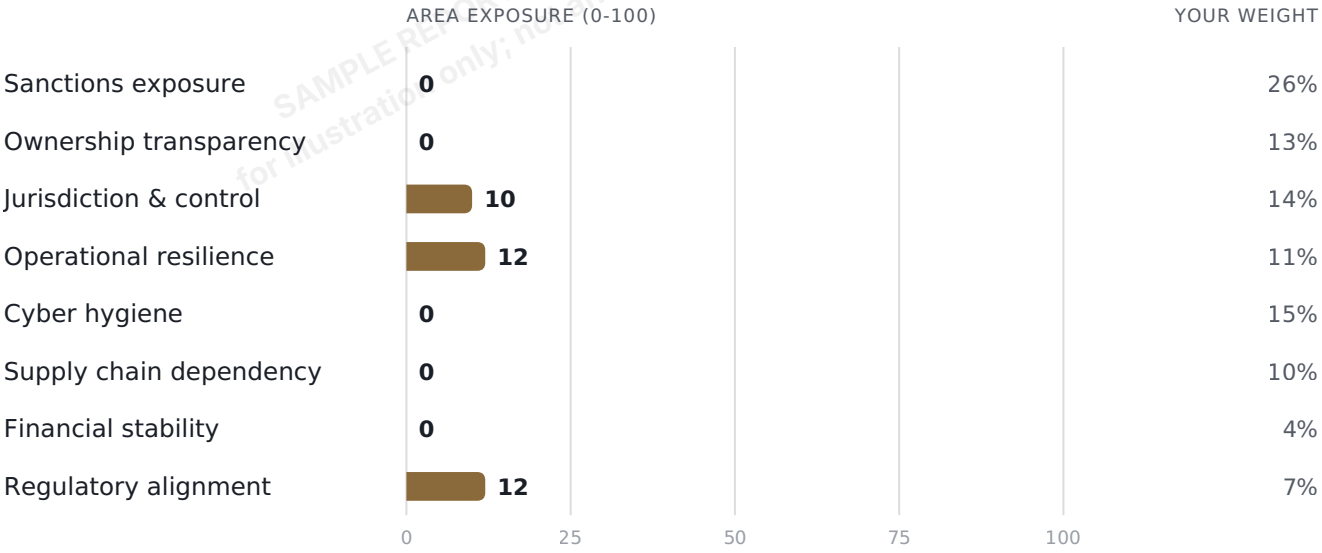
What drives this exposure

Your exposure index for Helvion Vault AG is driven mainly by Jurisdiction & control, Operational resilience and Regulatory alignment.

- **Jurisdiction & control** (area exposure 10, your weight 14%): for example: “Helvion Vault is headquartered in Zurich.”
- **Operational resilience** (area exposure 12, your weight 11%): for example: “The vendor's public documentation describes encrypted backups and geo-redundant storage, but it does not mention a documented business-continuity plan for the vendor's own operations or a continuity certification such as ISO 22301.”
- **Regulatory alignment** (area exposure 12, your weight 7%): for example: “Helvion Vault is established in Switzerland and does not name an EU representative or an EU-established subsidiary in its privacy documentation; support for EU customers is provided from Zurich.”

SAMPLE REPORT · fictional data for illustration only; not an assessment of any real vendor

Risk areas



Event timeline

The most significant documented events (up to 10), newest first. Items marked as context do not add to the exposure index.

DATE	EVENT	SOURCE
2026-10-20	A search of the consolidated sanctions lists of the United States, the European Union, the United Kingdom and the United Nations (as of 29 October 2026) returned no match for Helvion Vault, Helvion Holding or the named executives. context	Primary record · sanctions-demo.example [1]

DATE	EVENT	SOURCE
2026-09-02	Helvion Vault is headquartered in Zurich. Customer backup data is stored in its own data centres in Zurich and Geneva, with an optional second copy at a colocation partner in Frankfurt; no hyperscale cloud provider is used.	Vendor statement · helvion-demo.example [2]
2026-09-02	The vendor's public documentation describes encrypted backups and geo-redundant storage, but it does not mention a documented business-continuity plan for the vendor's own operations or a continuity certification such as ISO 22301.	Vendor statement · helvion-demo.example [3]
2026-09-02	Helvion Vault is established in Switzerland and does not name an EU representative or an EU-established subsidiary in its privacy documentation; support for EU customers is provided from Zurich.	Vendor statement · helvion-demo.example [4]
2026-04-14	Helvion Vault holds an ISO/IEC 27001 certificate and publishes an annual independent penetration-test summary. No publicly reported security incident or known exploited vulnerability was found for the vendor's products. context	Vendor statement · helvion-demo.example [5, 6]
2019-03-21	Helvion Vault AG is a privately held Swiss company owned by Helvion Holding AG, which is in turn held by its founders and two named Swiss family offices. The Swiss commercial register shows the full chain to natural persons; no hidden or unresolved ownership layer was found. context	Primary record · zefix-demo.example [7, 8]

Area analysis

Sanctions exposure

Area exposure 0 / 100 · your weight 26%

No matches across four sanctions regimes for the entity, its holding chain, or its executives (as of 2026-11-11).

Documented checks and context for this area

2026-10-20 · Primary record · sanctions-demo.example · Context [1]
A search of the consolidated sanctions lists of the United States, the European Union, the United Kingdom and the United Nations (as of 29 October 2026) returned no match for Helvion Vault, Helvion Holding or the named executives.

Items marked as context are documented events that do not add to the exposure index.

Ownership transparency

Area exposure 0 / 100 · your weight 13%

Beneficial ownership traced to its deepest registrable level via corporate registry filings (as of 2026-11-11).

Documented checks and context for this area

2019-03-21 · Primary record · zefix-demo.example · Context [7, 8]
Helvion Vault AG is a privately held Swiss company owned by Helvion Holding AG, which is in turn held by its founders and two named Swiss family offices. The Swiss commercial register shows the full chain to natural persons; no hidden or unresolved ownership layer was found.

Items marked as context are documented events that do not add to the exposure index.

Jurisdiction & control

Area exposure 10 / 100 · your weight 14%

2026-09-02 · Vendor statement · helvion-demo.example [2]
Helvion Vault is headquartered in Zurich. Customer backup data is stored in its own data centres in Zurich and Geneva, with an optional second copy at a colocation partner in Frankfurt; no hyperscale cloud provider is used.

SAMPLE REPORT · fictional data · Reference EB195F93
for illustration only; not an assessment of any real organisation

Operational resilience

Area exposure 12 / 100 · your weight 11%

2026-09-02 · Vendor statement · helvion-demo.example [3]
The vendor's public documentation describes encrypted backups and geo-redundant storage, but it does not mention a documented business-continuity plan for the vendor's own operations or a continuity certification such as ISO 22301.

Cyber hygiene

Area exposure 0 / 100 · your weight 15%

No active security-hygiene findings for this supplier (as of 2026-11-11).

Documented checks and context for this area

2026-04-14 · Vendor statement · helvion-demo.example · Context [5, 6]
Helvion Vault holds an ISO/IEC 27001 certificate and publishes an annual independent penetration-test summary. No publicly reported security incident or known exploited vulnerability was found for the vendor's products.

Items marked as context are documented events that do not add to the exposure index.

Supply chain dependency

Area exposure 0 / 100 · your weight 10%

No elevated-risk dependencies identified in this supplier's disclosed subprocessors and infrastructure (as of 2026-11-11).

Financial stability

Area exposure 0 / 100 · your weight 4%

No financial-stability risk indicators identified for this supplier (as of 2026-11-11).

Regulatory alignment

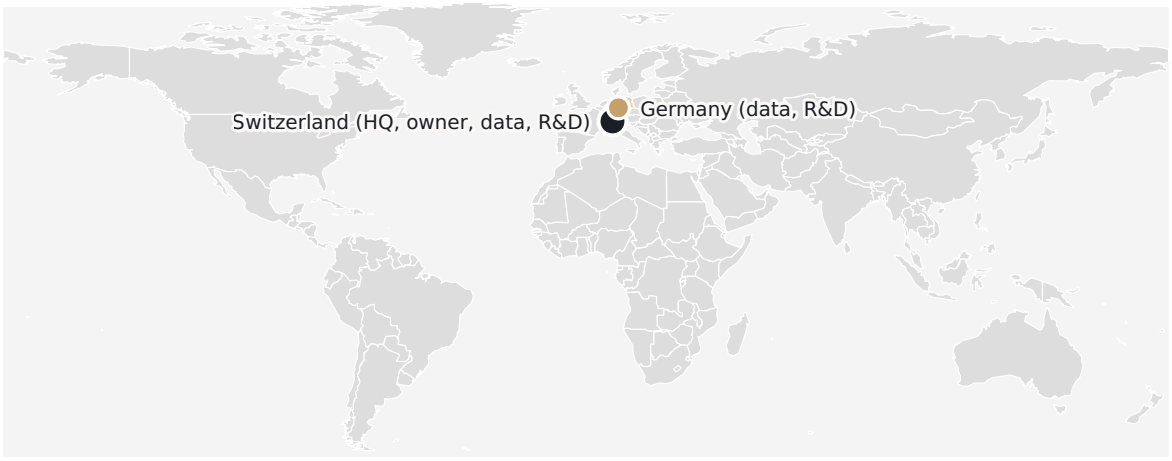
Area exposure 12 / 100 · your weight 7%

2026-09-02 · Vendor statement · helvion-demo.example [4]
Helvion Vault is established in Switzerland and does not name an EU representative or an EU-established subsidiary in its privacy documentation; support for EU customers is provided from Zurich.

SAMPLE REPORT · fictional data · Reference EB1957-2
for illustration only; not an assessment of any real organisation

Jurisdiction profile

Headquarters: Switzerland (Allied country). Ownership: Ownership structure verified against public records in Switzerland; no hidden or unresolved ownership layers were identified. R&D concentration: Switzerland 70%, Germany 30%. Data residency: Switzerland, Germany.



Headquarters	**Switzerland** · Allied country Close ally (e.g. US, UK); note — US law (including the CLOUD Act) may reach customer data regardless of where it is physically stored.
Ultimate ownership	**Switzerland** · Allied country Ownership structure verified against public records in Switzerland; no hidden or unresolved ownership layers were identified.
Data and processing locations	• **Switzerland** · Own data centres, Zurich and Geneva · Allied country • **Germany** · Colocation partner, Frankfurt · EU / domestic
R&D footprint	Switzerland 70%, Germany 30%
Can customer data leave the EEA?	Yes: at least one documented processing location is outside the EU/EEA (Switzerland).

SAMPLE REPORT · fictional data · Reference EB195F50
for illustration only · not an official document of any EU organisation

What these jurisdictions mean for you

- **Allied country**: Close ally (e.g. US, UK); note — US law (including the CLOUD Act) may reach customer data regardless of where it is physically stored.
- **EU / domestic**: National or EU jurisdiction — full protection of EU law.

What could change the assessment

Events that would be reflected in a later assessment of this vendor. They are examples, not a forecast.

Could increase your exposure

- **Sanctions exposure:** A new listing of the vendor, its owners or its directors on a sanctions or export-control list.
- **Cyber hygiene:** A newly disclosed, actively exploited vulnerability or a security incident affecting the vendor's products.
- **Jurisdiction & control:** A change in the legal systems that govern the vendor's headquarters, subsidiaries or data locations.

Could reduce it

- **Jurisdiction & control, Operational resilience, Regulatory alignment:** Independent documentation that the condition behind an existing finding has changed (for example a resolved ownership question or a remediated vulnerability) is taken into account in a later assessment.

Questions worth asking your supplier

- Request the vendor's DR/BCP documentation or ISO 22301 certification status.
- Request the vendor's GDPR Art. 27 EU representative or EU entity details.
- Which sanctions and export-control screening does the vendor perform on its owners, directors and sub-processors, and how often?

SAMPLE REPORT · fictional data · Reference E2F05F93
for illustration only; not an assessment of any real organization

What the full report contains

This sample covers two fictional vendors for a fictional client. A report for your organisation covers the vendors you choose and is built from your own context and weights.

For every vendor you order	An exposure index for your organisation, what drives it, a dated event timeline, an analysis of each of the eight areas, a jurisdiction profile with a map of headquarters, ownership, data and R&D locations, what could change the assessment, and questions worth asking the supplier.
Your context	Your answers about how you use each vendor and the weights you give each area shape every index. The report lists the configuration it was calculated from.
Sources	Every finding in your report cites its source, and Appendix A lists them all. This sample shows three of them as examples.
Assessment perspective	EU/NATO: EU/EEA countries count as home; allied countries are assessed for legal reach over data. The configuration page of a real report states it.
Comparison with other vendors	Orders include a relative comparison with the other vendors we assess; it is left out of this sample.
Updates	With a subscription the assessment is refreshed every month, and the report you download always shows the date it was prepared.

SAMPLE REPORT · fictional data · Reference FB195F93
for illustration only; not an assessment of any real organisation

Methodology and disclaimers

Methodology in brief: eight areas (sanctions exposure, ownership transparency, jurisdiction and control, operational resilience, cyber hygiene, supply chain dependency, financial stability and regulatory alignment). Each documented finding contributes to the exposure of the area it belongs to, on a scale of 0 to 100. The context you provided changes how much a given type of finding weighs for your organisation, and the area exposures are combined using the weights you selected into the Client Exposure Index. Legal status flags are shown separately and are not part of the index. Model version: **E-1.0**. Source-cited principle: every factual statement is backed by a cited source, shown next to the finding and listed in full in Appendix A.

Jurisdiction categories follow the assessment perspective shown in the assessment configuration.

What this report measures, and what it does not: the report assesses structural geopolitical, ownership and operational exposure. It is not a product security audit, not a breach prediction, and not an investment or contract-termination recommendation. It does not state whether a vendor complies with any law or standard (including GDPR, NIS2, DORA or national cybersecurity legislation).

Review of findings: findings are collected from publicly available sources and reviewed by analysts before they are used in an assessment.

Disclaimers

> This index represents the customer's individual exposure to the vendor based on the risk dimensions and weighting selected for this assessment. It is not a universal rating of the vendor.

This is an individual assessment prepared on the order of the organisation named on the cover and issued to that organisation only. It may not be shared outside it. The legal terms applicable to this document are the terms of service accepted at the time of the order.

Point in time

This report reflects sources checked through **11 November 2026**. Every fact is dated to the underlying event, not to the day it was found. Data references: aad51681a5, dc1bf1d714.

Contact

For questions about this report or to dispute a specific finding: support@vendorexposure.com.

Frequently asked questions

Does a lower index mean the vendor is safe to use? No. The index covers the eight areas described above for your organisation's context. It does not cover product security, operational quality or anything outside this methodology.

Does a higher index mean we have to stop using the vendor? No. This report never recommends replacing or terminating a vendor. It documents the findings and shows how they weigh for you.

Why does another organisation see a different number for the same vendor? Because the index depends on the context and the weights chosen for each order. The underlying findings about the vendor are the same.

What happens if a finding is wrong or out of date? Contact us at the address above and we will review it.

Appendix A: sources per vendor

In your report, every source behind every finding is listed here, with the number that appears in square brackets next to the finding. This sample cites 19 sources; three are shown below as examples of how a source is described: its title, its domain, its type and the date we checked it.

TYPE	TITLE	SOURCE	CHECKED
Primary record	Sanctions list aggregator - search result, 29 October 2026	sanctions-demo.example	2026-10-29
Vendor statement	Kestrel Mobile Security - subprocessor list	trust.kestrel-demo.example	2026-10-29
Press tier 2	Tech Ledger - Kestrel expands Shenzhen development centre	techledger-demo.example	2026-10-29

SAMPLE REPORT · fictional data · Reference EB195F93
for illustration only; not an assessment of any real organisation

Appendix B: glossary

Client Exposure Index	A number from 0 to 100 that expresses the exposure of your organisation to one vendor, calculated for this order from your context and weights. It is not a universal rating of the vendor.
Area exposure	The exposure of one of the eight areas for one vendor, from 0 to 100, after taking your context into account.
Weight	The share, in percent, that you assigned to an area. The weights sum to 100%. An area with weight 0 is not included.
Importance	How significant a vendor is within your portfolio. It determines how much the vendor counts towards the portfolio figure.
Portfolio exposure	The average of the vendors' exposure indices, weighted by the importance you assigned to each vendor.
Legal status flag	A notice shown above the index when an official source documents a legal status of the vendor (for example a sanctions listing). It is independent of your weights.
Context	Your answers about how you use each vendor. They change how much a type of finding weighs for you but never remove a finding.
Finding	A dated, documented event or fact about the vendor that is backed by at least one cited source.
Source types	Primary record: an official register, filing or notice. Technical: a technical database or advisory. Press tier 1 and tier 2: news organisations, in descending order of editorial standing. Vendor statement: the vendor's own published material. Crowdsourced: a community-maintained dataset.
Sanctions exposure	Whether the vendor, its owners or key people are subject to sanctions or export controls.
Ownership transparency	How clearly the vendor's real owners can be identified and whether control has changed.
Jurisdiction & control	Which legal systems govern the vendor, its data and its operations, and what that means for you.
Operational resilience	How well the vendor can keep operating: concentration, continuity planning, past outages.
Cyber hygiene	The vendor's security track record: known exploited vulnerabilities, patching, breaches, certifications.
Supply chain dependency	Who the vendor itself depends on: subprocessors, cloud providers, open-source and hardware.
Financial stability	Signals that the vendor may be unable to keep supporting you.
Regulatory alignment	Fit with the regulations that matter to you: data protection, NIS2/DORA, official warnings.

SAMPLE REPORT · fictional data · for illustration only · not an assessment of any real organisation