CYBERRANK

PRODUCT BROCHURE · 2026

THIRD-PARTY CYBER RISK INTELLIGENCE

Your next cyber incident will likely come through a vendor.

CyberRank rates any organisation's security, privacy and AI risk from just its web address, in 10 to 60 minutes, without questionnaires or access to its systems. Built for DORA, NIS2, the EU Cybersecurity Act, GDPR and the EU AI Act, and for third-party rules in the US, Middle East, India, Indonesia, Singapore and Australia.

BBB IISRI® EXTERNAL RATING

Satisfactory · low risk

vendor-example.com · illustrative



Security	Privacy	Data leaks	Controls	AI	Quantum
71%	78%	64%	82%	69%	58%

100,000+ assessments created

17,846,550,965 leaked credentials tracked

3,338 data breaches discovered

5,600 vendors tracked

BUILT FOR

Financial institutions · Government agencies · Healthcare & critical infrastructure · Insurers · MSSPs · Enterprises & SMBs

Powered by IISRI® · ISO/IEC 27001 & 42001 certified · figures as of Oct 2026

cyberrank.ai

Every vendor you add widens your attack surface.

Attackers increasingly reach organisations through their suppliers. Yet most vendor risk management still runs on questionnaires, spreadsheets and annual reviews: slow to complete and out of date the day they are filed. Meanwhile DORA, NIS2, the EU Cybersecurity Act (CSA), GDPR, the EU AI Act and SEC rules expect continuous, evidenced third-party oversight.

Minutes, not weeks

A complete security, privacy and AI rating from a single URL in 10–60 minutes, so onboarding never waits on a questionnaire.

Less manual effort

Collection, analysis and monitoring are automated, freeing your team for decisions rather than data gathering.

Fewer costly breaches

Spot weak TLS, leaked credentials and risky policies early, before they become your incident and your fine.

Spend where risk is

Severity-ranked findings and impact tiers show which vendors, and which fixes, deserve attention first.

How it works

100% non-invasive · no agents · no access needed

1

Enter a URL

Type a vendor's web address. CyberRank finds the company and every public subdomain.

2

Evidence is assessed

Deterministic checks, probabilistic models (incl. pinned open-weight AI) and heuristics (p. 6) assess:

Network data · Scan data · Policies · Security setup · Cryptography · Certificates · Legal terms · Breach data · Dark web · **AI use**

3

Act on the results

Within 10–60 minutes: an IISRI® rating from D to AAA, ranked findings with fix guides, and an audit-ready PDF.

50+ subdomains assessed per organisation, not just the homepage. Staging servers, admin portals and forgotten APIs are where exposure hides.

Third-party cyber risk is a legal duty, worldwide.

Regulators expect you to assess, monitor and manage supplier cyber risk. CyberRank provides the evidence.

European Union EU

DORA: ICT third-party risk management and a register of ICT providers.

NIS2: supply-chain security as a required risk measure.

EU Cybersecurity Act (CSA): EU certification of ICT products and services.

Also: GDPR (Art. 28 processors) · EU AI Act

United States US

SEC cyber disclosure rules: disclose how third-party provider risk is managed.

NYDFS 23 NYCRR 500: third-party service provider security policy (§500.11).

Interagency TPRM Guidance (Fed, FDIC, OCC): vendor life-cycle risk management.

Also: HIPAA business associates · CMMC 2.0

Middle East KSA · UAE

Saudi NCA ECC: a dedicated third-party cybersecurity domain.

SAMA Cyber Security Framework: third-party and outsourcing security for financial institutions.

UAE Information Assurance Regulation: third-party security controls.

Also: Dubai DESC ISR

India IN

RBI Outsourcing of IT Services: due diligence and ongoing monitoring of IT providers.

SEBI CSCRF: vendor and third-party risk management.

IRDAI Cyber Security Guidelines: third-party security for insurers.

Also: DPDP Act 2023 (data processors)

Indonesia ID

OJK Reg. 1/2026 (IT governance, banks): due diligence and reassessment of IT providers.

POJK 11/2022: IT implementation by banks, incl. IT service providers.

UU PDP (Law 27/2022): controllers answer for their processors.

CyberRank scores UU PDP compliance natively

Singapore SG

Cybersecurity Act (amended, in force Oct 2025): binding commitments from CII vendors.

MAS TRM Guidelines: third-party and vendor risk management.

MAS Outsourcing Guidelines: due diligence and monitoring of service providers.

Also: PDPA (data intermediaries)

Australia AU

APRA CPS 234: assess third parties' information security capability.

APRA CPS 230: manage material service providers (since 1 July 2025).

SOCI Act: supply-chain hazards in critical-infrastructure risk programs.

Also: Privacy Act 1988 (APP 11)

How CyberRank helps

- Pre-contract due diligence in 10–60 minutes
- Continuous monitoring with alerts
- Impact tiers mapped to DORA critical / important
- Fourth-party and combined supply-chain risk
- Audit-ready reports and evidence registers

Plus supplier requirements in security, privacy and AI standards

ISO/IEC 27001 A.5.19–5.23 · **PCI DSS v4.0** Req. 12.8 · **NIST CSF 2.0** GV.SC · **NIST SP 800-53** SR family

SOC 2 CC9.2 · **ISAE 3402** service orgs · **ISO/IEC 27701** processors · **ISO/IEC 42001** A.10

Simplified for orientation, not legal advice. CyberRank supports these obligations; it does not by itself make an organisation compliant.

One report. The full external picture.

Real output from a CyberRank assessment of an education-sector platform, run on 22 Oct 2026 (organisation name withheld). The full report runs to 83 pages and is generated automatically.

IISRI® EXTERNAL RATING

B **Moderate**

185 of 360 points · method 2026.07



"Many specific control weaknesses have been noted. Major additional work is highly recommended."

SCOPE AND COVERAGE

57 subdomains scanned

58 hosts observed

100% coverage

0 access required

Aspect scores

100% = best

Privacy	43%
Vulnerabilities	20%
Credential exposure	45%
Data breach history	100%
Data residency	100%
Legal terms	100%
Certifications	24%

Other outputs

Quantum security	54 high-risk · PQC on 19 domains
AI & EU AI Act	AI use & tier as probability
Fourth-party vendors	15 rated · lowest B
Data sovereignty	Netherlands / EU courts
Cloud infrastructure	AWS
Vulnerabilities	1 high · 4 medium · 7 low

The AI lens is new and was not part of this sample run.

Sector benchmark

This vendor	51
Sector average	56
Top 10%	66

Education · 100 peers · 2026 Q3

Priority actions

HIGH	Remediate SSL/TLS weaknesses	2–3 days
MED	Update privacy policy & disclosures	1 week

Projected after remediation: B → AAA

219 exposed account records, 44 with passwords

14 privacy-policy issues, each explained

19 hosts with findings, incl. staging & admin

1 of 2 customer-protection clauses in its terms

Twelve risk lenses in every assessment

Each lens is scored, explained in plain language and paired with remediation guidance. The orange line shows what it found in the sample report. Every report adds sector benchmarking, priority actions with effort estimates, a projected rating and full evidence registers for auditors.

01 Privacy

Policy split into 15+ areas, cookie consent, GDPR and Indonesia's UU PDP indicators, with rewrite suggestions.

▸ 14 issues, e.g. bundled consent that is hard to refuse

02 Vulnerabilities

TLS, certificates, headers, email security and known CVEs on every subdomain, severity-ranked with copy-paste fixes.

▸ 13 finding types across 19 hosts, incl. staging & admin

03 Credential exposure

Leaked emails, usernames and passwords from breach compilations, infostealer logs and dark-web sources.

▸ 219 records; 41 match infostealer patterns

04 Data breach & leak history

Checks breach databases worldwide for past incidents and what data was exposed, with a full timeline.

▸ No public breach events on record

05 Data sovereignty

Finds the governing law and courts in a supplier's terms and compares them with the jurisdictions you accept.

▸ Netherlands / EU courts identified

06 Data residency

Maps where public systems are hosted and checks them against your preferred countries.

▸ 58 hosts geolocated

07 Legal terms & conditions

Reads login and payment-portal terms for customer-protection clauses: data protection and breach notification.

▸ 1 of 2 clauses found; no breach-notice clause

08 Quantum security BETA

Flags cryptography vulnerable to future quantum attacks and detects post-quantum (PQC) algorithms in use.

▸ 54 high-risk findings; PQC seen on 19 domains

09 Certifications

Detects ISO 27001/27701, SOC 2, PCI DSS, HIPAA, NIST and more, verified or claimed. Vendors can upload evidence.

▸ ISO/IEC 27001 detected and approved

10 Fourth-party vendors

Identifies and rates your vendor's own suppliers, flagging the weakest links in the chain.

▸ 15 suppliers rated, from B to AAA; 4 need a look

11 Cloud infrastructure

Identifies cloud providers from DNS, IP ranges, MX and NS records, revealing concentration risk.

▸ AWS detected

12 AI & EU AI Act NEW

Estimates whether a vendor uses AI, which AI Act tier its product falls in (incl. Annex III high-risk) and whether visible obligations are met.

▸ Read as Unlikely · Possible · Likely · Almost certain (%)

One rating for every vendor. One risk number for your whole supply chain.

THE PROBLEM

Existing tools don't add up: CVSS scores single flaws, questionnaires rely on self-reporting, and privacy, AI and quantum exposures have no common scale.

THE APPROACH

An ISO 31000-aligned model in four explicit steps. Every step is reproducible and every number is comparable across organisations and portfolios.

THE REGULATORY FIT

DORA, NIS2, the EU Cybersecurity Act (CSA), GDPR and the AI Act, plus supply-chain requirements in ISO/IEC 27001, ISAE 3402, NIST SP 800-53 & 800-161, PCI DSS and NIST CSF.

1 Observe

Continuous external signals, collected without touching the organisation's systems:

Vulnerabilities · Privacy compliance · Credential & data leaks · Data sovereignty · Data residency · Terms of use · AI · Quantum

2 Rate

A full point budget, split evenly into security and privacy. Weaknesses deduct capped demerits; certified controls (ISO 27001, 27701, SOC 2, ISAE 3402, PCI DSS) add capped credits. The net score maps to AAA–D and reflects the organisation's own posture only.

3 Score the risk

Likelihood = threat probability (sector, size, internet exposure) × weakness (the rating). Impact is the tier you assign. Risk = normalised likelihood × impact, reported as a score and a band.

4 Combine

Vendors and sub-vendors are discovered automatically and rated with the same pipeline. Their risk folds into yours, damped by distance in the chain.

Optional questionnaires add a second, bounded evidence channel. A vendor's weakness never changes your own rating.

Risk heat map

impact tier × likelihood = band

Impact \ Likelihood	Very unlikely	Unlikely	Possible	Likely	Very likely
T1 · Critical	Low	Medium	High	Critical	Critical
T2 · High	Low	Medium	Medium	High	Critical
T3 · Medium	Low	Low	Medium	Medium	High
T4 · Low	Low	Low	Low	Low	Medium

Pick the row for the vendor's impact tier (Medium is the default at onboarding), find its likelihood column, and read the band. The heat map is the qualitative view; the continuous risk score remains primary.

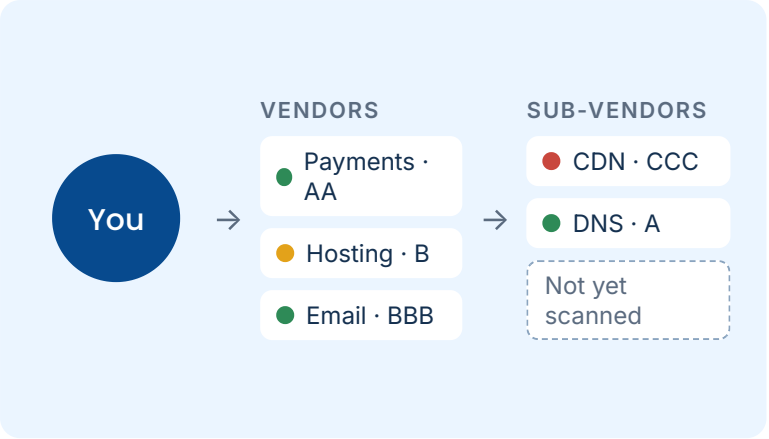
The IISRI® rating scale

higher grade = lower weakness = lower likelihood

AAA	AA	A	BBB	BB	B	CCC	CC	C	D
Excellent	Very good	Good	Satisfactory	Sufficient	Moderate	Insufficient	Very insufficient	Poor	Very poor

Your rating describes you. Your combined risk describes your supply chain.

Every vendor and sub-vendor is rated with the same pipeline as you are. A weak vendor never lowers your own rating, which stays attributable to your posture. But an exploited vendor can open an attack path into your systems, so its weakness enters your combined risk, damped by how far away it sits in the chain.



Individual risk

Low

Your own posture, as if you had no suppliers. Fit for external presentation.

Combined risk

Medium

You plus every vendor and sub-vendor. The number to manage against.

Illustrative example.

Combined risk: the “at least one adverse event” composition, applied recursively through the chain

$$R(N) = 1 - (1 - o_N) \cdot \prod_{s \in \text{suppliers}(N)} \left(1 - R(s) / (f + d(s))^2 \right)$$

o_N a node's own individual risk, from its rating, threat probability and impact tier.

$R(s)$ a supplier's effective risk, computed the same way from its own suppliers.

$d(s)$ hops from the centre; each supplier one step further out is damped more.

f the transmission fraction you configure; a larger f shrinks every supplier's contribution.

Impact tiers you assign to each vendor

- **T1 Critical**: failure immediately stops a critical service or causes a serious regulatory breach. DORA: critical.
- **T2 High**: essential, but a temporary loss can be bridged. DORA: important.
- **T3 Medium**: supports normal operations. The default at onboarding.
- **T4 Low**: minimal or no operational impact.

Why you can rely on it

Standards-grounded: ISO 31000, ISO/IEC 27001, 27701 & 42001, NIST SP 800-30 & 800-53, DORA, NIS2 and the EU Cybersecurity Act (CSA).

Certified operator: independently audited ISO/IEC 27001 and ISO/IEC 42001 management systems.

Human in the loop: users report inaccuracies and appeal findings; feedback tunes detection confidence.

Honest about limits: vendor compromises are treated as independent, some detections are heuristic, and the continuous score is primary.

An organisation's own excellent rating does not certify its supply chain. **Only the combined risk does.** The dashboard shows six domains for you and every (sub-)vendor: Security, Privacy, Data leaks, Controls, AI and Quantum.

From one-off check to 24/7 watchtower

The report is where it starts. The platform keeps every vendor's rating current and builds VRM into the way your team already works.

Continuous monitoring

Daily re-scans across all modules, darknet monitoring and email alerts the moment a vendor's posture slips.

Rating history & trends

A month-by-month timeline of every vendor's rating, to evidence improvement or catch decline.

AI-powered questionnaires

Build from scratch or a template, or upload an existing PDF for AI to structure. Answers and evidence feed the internal rating.

Vendor self-service portal

Vendors see their findings, upload certificates and assurance reports, and request re-evaluation.

Benchmarking & critical suppliers

Compare vendors with sector peers, get substitution recommendations and classify critical suppliers for DORA.

Individual risk & data monitoring

Scan employee email addresses for breached credentials, with ongoing alerts when new leaks appear.

REST API & webhooks

Pipe ratings and alerts into GRC, SIEM, procurement and ticketing tools such as ServiceNow and Jira.

Audit-ready PDF reports

Executive summary to evidence register, ready for procurement, the board and auditors. Unlimited users.

How teams use CyberRank

Risk, procurement & compliance

- Vet vendors before you sign
- Monitor critical suppliers
- React fast to supply-chain breaches
- Evidence DORA, NIS2, CSA and ISO 27001 oversight

MSSPs & consultants

- Assess client estates at scale
- Turn findings into remediation work
- Automate incident response via API
- One shared credit pool for the team

Insurers & underwriters

- Rate applicants from a URL
- Price cyber cover on evidence
- Watch the portfolio for drift
- Spot aggregation risk in shared suppliers

Start free Create a free account to see how your own organisation rates, or try the post-quantum cryptography assessment and medical-sector breach check tools at cyberrank.ai.

Pay for vendors, not seats.

Transparent credit-based pricing. No subscriptions required, no hidden fees, unlimited users.

1 credit = $1
used across every feature

THE INSTANT CHECK

Assessment

20 credits / vendor

One-off · results in 10–60 minutes

- ✓ Security assessment
- ✓ Privacy assessment
- ✓ Data leak history
- ✓ Compliance identification

BEST CHOICE

24/7 WATCHTOWER

Monitoring

30 credits / vendor / month

Was 600 credits: 95% off

- ✓ Everything in Assessment
- ✓ Daily re-scans & email alerts
- ✓ Darknet monitoring
- ✓ Compliance updates

FOR BUILDERS

API access

500 credits / month

Monthly · full programmatic access

- ✓ Full REST API
- ✓ Real-time webhooks
- ✓ Darknet monitoring
- ✓ Automated procurement

Example: 35 vendors one-off assessments (700 cr) + 5 vendors monitored for 12 months (1,800 cr) **$2,500 / yr**

Credits are valid for 12 months and work across every feature. Invoices are issued in USD.

CyberRank vs. legacy solutions: more than price

	CyberRank	UpGuard	SecurityScorecard	BitSight
Monitoring per vendor, per year	**$300–400**	$480–960	$1,500–2,000	$2,000–2,500
Licence based on	**Credits**	Vendor + user	Vendor + user	Vendor
User licences	**Unlimited**	Strictly limited	Strictly limited	Strictly limited
Privacy risk detection	**✓ Included**	× Not covered	× Not covered	× Not covered
Quantum / PQC readiness	**✓ Included**	× Not covered	× Not covered	× Not covered
AI & EU AI Act risk	**✓ Included**	× Not covered	× Not covered	× Not covered

Also included with CyberRank: Fourth parties · Data residency · EU data sovereignty · Legal clause detection · Vendor evidence uploads · Questionnaire automation

> “For any company seeking certification and security policy advancement, partnering with IISRI® is a definite win.”

Matt Scarmardo · CIO, Stellar Elements, an Amdocs company

CUSTOMERS INCLUDE

BKR	PLN Batam	Compass Group	Daifuku	Medtech	Atturra	Recare	Lucidity
Blueoak	CyberVade	Banjo Health	Devoli	Conporto Health	NZ Doctor	iProteksi	MTM

A PT PLN Batam

The Indonesian utility earned an A rating with very low risk, reported as the country's highest cybersecurity level at the time.

iNews Batam and RRI, 18 Aug 2026

“CyberRank has more complete features compared to competitors at a much more affordable cost, including valuable UU PDP compliance assessment.”

PLN Batam commissioner, as reported by RRI

BUILT ON RECOGNISED STANDARDS

ISO/IEC 27001
Certified 2026 · information security

ISO/IEC 42001
Certified 2026 · AI management

ISO 31000 · NIST
Risk model, SP 800-30 / 53

GDPR & EU AI Act
Privacy and AI regulation

See how your vendors rate today.

Create a free account and have your first assessment within the hour, or book a demo and we'll walk your team through a live report.

Create free account · cyberrank.ai/vas/register

Book a demo

Web
cyberrank.ai

Email
support@cyberrank.ai

Office
Level G, 26 Hobson Street
Auckland City 1010, New Zealand