VCRI
THE VALUE CHAIN RISK INSTITUTE

VCRI LEARN · ABOUT THE INSTITUTE

Why VCRI?

What The Value Chain Risk Institute is, the problem it exists to fix, and how to use what it has built.

Joshua Marpet and Cairn Viktor

VCRI
THE VALUE CHAIN RISK INSTITUTE

THE PROBLEM

Vendors are grading their own homework.

Questionnaires, annual audits and self-attestation decide whether we trust the companies we depend on. Those tools were designed for a world that no longer exists.

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

WHY THE OLD WAY BREAKS

Three problems with vendor assessment today

Questionnaires don't verify

Vendors self-report. Nobody checks. The incentive is to check every box, not to tell the truth.

Audits are snapshots

An annual audit measures one moment. Attackers work continuously. The gap is measured in months.

Every buyer asks differently

Each customer sends its own form, so the same vendor answers the same questions again and again.

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

WHO WE ARE

A neutral nonprofit

The motto: inside data, not guesses.

What VCRI is

The Value Chain Risk Institute is a nonprofit and a neutral party.

Its purpose: a trusted clearinghouse for vendor security posture evidence.

How it behaves

“We grade evidence, we do not sell your data, and no vendor can buy a better result.”

Methods are open, so anyone can check how a result is reached.

valuechainrisk.org/learn · CC BY 4.0

THE METHOD

The Cyber Assurance Matrix (CAM)

Six TIPPSS dimensions

Trust, Identity, Privacy, Protection, Safety, Security.

From the TIPPSS framework (IEEE/UL 2933).

Six PPTDF-AI asset classes

People, Processes, Technology, Data, Facilities, AI.

Adopted by the VCRI board on March 16, 2026.

Five maturity levels

Each of the 36 cells gets a level from 1 (Initial) to 5 (Optimizing).

Based on the Capability Maturity Model Integration (CMMI) scale.

valuechainrisk.org/learn · CC BY 4.0

THE CORE IDEA

The gap is the risk

Traditional risk asks you to guess likelihood and impact. CAM asks what is unverified.

Required level

How mature a vendor needs to be in each cell, given what you depend on it for.

→

Actual level

How mature the evidence shows the vendor really is.

→

The gap

= risk signal

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

OPEN SCORING

BeaconScore: check the arithmetic

Free, runs in your browser, licensed CC BY 4.0. Score a vendor, or yourself.

Published rubrics

Six rubrics, one per PPTDF-AI asset class, each scored 0 to 5.

Every weight is public.

Clear grades

Grades A through F.

A very weak dimension caps the grade, so one strength cannot hide a failure.

Changes in the open

Release notes record every rubric change and why, so results can be re-run and compared.

VCRI
THE VALUE CHAIN RISK INSTITUTE

EVIDENCE, NOT ANSWERS

Beacon Collector (beta)

Open source. Beta scores use a draft method and are labeled that way.

Runs on your machines

Reads the security tools you already run: scanner results, SBOMs, identity-provider exports and more.

Your evidence stays with you.

Sealed and scored

Every item is hashed; the package carries one fingerprint and a signature. Change one byte and verification fails.

Scored against the open rubrics on a one-page results view.

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

FREE TOOLS

Built to be used, not sold

Cyber Resilience Act builders

Cyber Manual Builder, TARA Builder, and Context and Conditions of Use Builder.

Run in your browser; nothing uploaded.

AIBOM Constellation Inventory

Lists everything an AI agent depends on as a CycloneDX AI bill of materials.

Open source, Apache-2.0.

AI Cognitive Security Framework

Can an AI system be trusted with what it reads, remembers and does?

7 dimensions, 40 questions.

Kits for small organizations

Small businesses, small utilities, community banks and credit unions, rural hospitals.

Plus a plain-language glossary.

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

OPEN RESEARCH

State of the Supply Chain

A quarterly report on open-source supply-chain risk, with methodology and data you can check.

13.1 million

open-source packages classified in the Q3 2026 issue, the entire published corpus.

2 to 3×

how far the headline abandonment number moves between equally defensible definitions. The honest unit is a band.

Open data

Band table, watch list and verification evidence published with every issue, plus the mistakes caught along the way.

Source: VCRI, State of the Supply Chain Q3 2026, valuechainrisk.org/state-of-supply-chain/

valuechainrisk.org/learn · CC BY 4.0

VCRI
THE VALUE CHAIN RISK INSTITUTE

GET INVOLVED

What to do Monday

- Score one vendor, or your own team, with BeaconScore at valuechainrisk.org/scorer.
- Take the two-minute Security Tools Poll, so the Beacon Collector learns the most-used tools first.
- Find your local security groups, or share a field kit, from valuechainrisk.org/community.
- Read a State of the Supply Chain report and send a correction if you find one.
- Reach the Institute at info@valuechainrisk.org.

valuechainrisk.org/learn · CC BY 4.0

VCRI

THE VALUE CHAIN
RISK INSTITUTE

Free to use, teach and share.

This deck is part of the VCRI Learn series. Use it in your class, your team meeting or your chapter, with credit to The Value Chain Risk Institute.

valuechainrisk.org/learn

valuechainrisk.org/learn · CC BY 4.0