SAMPLE REPORT · DEMO DATA

3HUE
Executive Consulting

AI & SECURITY RISK POSTURE SNAPSHOT

Big Venture Incorporated

Where the organization stands on AI governance and security posture, what it should do in the next ninety days, and who owns each move. Ten business days, one read leadership can act on.

Prepared for
Chief Operating Officer and Head of Technology
Big Venture Incorporated · Energy · 2 entities

Prepared by
3HUE Executive Consulting · named vCISO
Scan of September 19, 2026 · readout September 26, 2026

Scope
One business unit, one AI program · AWS Production, Azure Production, Microsoft 365

Classification
Confidential to the client. This copy uses the Big Venture Incorporated demo workspace; every figure is sample data.

Posture 71 of 100, grade B−. Governed AI is three decisions away.

Big Venture runs 642 cloud resources across AWS and Azure with 629 open findings, none critical. The security program is 70% implemented against its control baseline and SOC 2 is 59% passing on live evidence. The AI program has five use cases in flight and no governing layer yet: no acceptable-use policy, no system inventory, no human-review rule. That gap, not the cloud findings, is the first thing to close.

POSTURE SCORE

71/100

Grade B− · ▲ 1 vs last scan

OPEN FINDINGS

629

0 critical · 293 high · 270 medium · 66 low

OPEN POA&M

9 of 10

1 past 90 days · 5 aging past 30

BASELINE IMPLEMENTED

70%

23 applicable controls · 2 entities

WHAT IS WORKING

- Identity is centralized; MFA is enforced for all 312 employee accounts.
- Cloud scanning runs daily; every finding carries an owner and a due date.
- SOC 2 evidence is mapped for 11 of 12 in-scope controls and refreshed by each scan.
- Incident response has a declared process, with 0 open incidents of 1 declared this year.

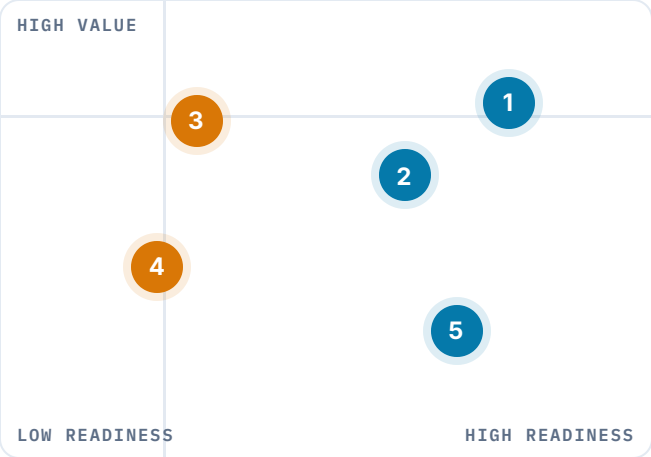
WHAT IS NOT

- Five AI use cases run without a policy, an inventory or a review rule.
- Two third-party contractor groups operate without MFA (POAM.2026.003).
- Privileged cloud credentials rotate manually; one set is 410 days old.
- Audit logging is off in two secondary regions, so 14% of resources have no trail.

The three decisions. Approve the AI acceptable-use policy and the human-review rule (week 1). Fund credential rotation and contractor MFA as one remediation sprint (weeks 2–5). Pick the lane for the program: keep running it in Client Vision, or hand the seat to 3HUE (week 6).

Five use cases, scored on value and readiness.

Each use case was scored with its business owner on expected value (cost out, revenue in, risk down) and on readiness (data, controls, vendor terms, human oversight). Top right goes first. Top left is where the value is but governance has to come first. The bottom row waits.



#	USE CASE	OWNER	VALUE	READY
1	Field maintenance assistant (work-order summaries)	Operations	8.5	8.0
2	Customer support copilot (tier-1 responses)	Customer Care	7.0	6.5
3	Contract review (supplier terms, clause extraction)	Legal	8.0	3.5
4	Load forecasting model (regional demand)	Planning	5.5	3.0
5	Internal knowledge search (policies, runbooks)	IT	4.0	7.5

Reading the map

GO NOW

1 and 5 can run under the new policy in the first month. Both use vendor models with enterprise terms already in place; the remaining work is a human-review rule and logging.

GOVERN FIRST

3 touches supplier contracts and personal data; it needs a data-handling decision and a DPIA before the pilot resumes. 2 needs a customer-facing disclosure and an escalation path.

HOLD

4 depends on a data pipeline that has no lineage and no owner. Value is real but a model on ungoverned data is a risk, not an asset. Revisit at the 90-day review.

Eight components. Three in place.

The same eight components an auditor, a board or an enterprise customer asks for first. Status reflects what could be shown at the readout, not what is planned.

COMPONENT	STATUS	FINDING	OWNER · DUE
AI acceptable-use policy	MISSING	No approved policy; a draft from IT has not been reviewed by Legal or HR.	General Counsel · Oct 10
AI system inventory and risk register	MISSING	Five use cases known to the Snapshot team; none recorded with owner, data touched or residual risk.	Head of Technology · Oct 17
Human review and override rules	MISSING	Support copilot responses go to customers without a review step above a confidence threshold.	Customer Care · Oct 17
Model lifecycle framework	PARTIAL	Vendor models are versioned by the vendor; no internal validation or retirement step.	Head of Technology · Nov 14
Data governance for AI	PARTIAL	Classification exists for the data warehouse; training and inference data for use cases 3 and 4 are unclassified.	Data lead · Nov 21
Third-party AI oversight	IN PLACE	Two vendors under enterprise terms with data-processing agreements and no training on client data.	Procurement · maintained
AI incident response	IN PLACE	The incident plan names AI failure modes and bias events since the June revision; the contact tree is outdated (POAM.2026.007).	IR lead · maintained
Decision rights and review cadence	IN PLACE	The technology steering committee owns AI decisions and meets monthly; the AI item is now standing.	COO · maintained

REGULATORY READ

No use case meets the EU AI Act's high-risk definition today; the load forecasting model would if it fed grid-operations decisions. US state privacy law applies to use cases 2 and 3 through customer and supplier personal data. Document the classification now so the answer is on file.

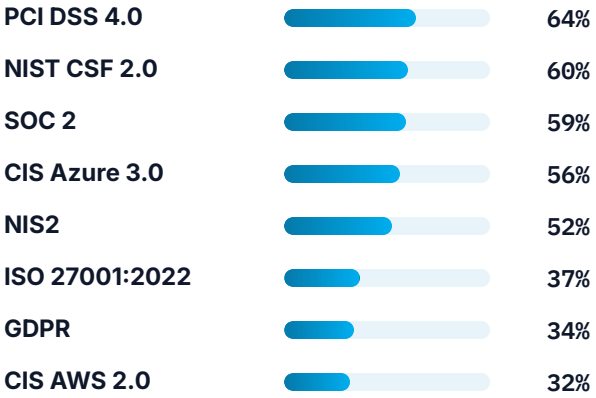
WHAT CLOSES THE GAP

Policy, inventory and review rule are three documents and one steering-committee decision. 3HUE drafts all three from the templates in the AI governance pack; approval is the long pole. Target: all eight components in place by day 60.

One scan, eight frameworks, one number.

CloudSignals scanned 642 of 662 resources across AWS Production and Azure Production on September 19 (2,835 checks, Prowler-based engine with AI correlation). Every framework below reads from that one scan, so the posture the board sees and the pass rate the auditor sees never disagree.

COMPLIANCE SNAPSHOT · PASS RATE



Severity-weighted pass ratio across 2,835 checks; one formula, every view.

FINDINGS BY PROVIDER



0 critical · 293 high · 270 medium · 66 low. The high findings concentrate in identity (credential age), storage (public reachability, missing default encryption) and logging.

TOP RISKS · ROAR, LIKELIHOOD × IMPACT

1	Privileged cloud credentials without rotation AWS Production	CRITICAL	**20** L4 × I5
2	Publicly reachable storage with sensitive data Azure Production	HIGH	**16** L4 × I4
3	CI/CD repos without branch protection AWS Production	HIGH	**16** L4 × I4
4	Management ports open to the internet Azure Production	MEDIUM	**9** L3 × I3
5	Audit logging disabled in secondary regions AWS Production	MEDIUM	**8** L2 × I4

Ninety days, three phases, named owners.

The plan is written into the Client Vision tenant that was onboarded during the Snapshot, so every item below is already a POA&M entry or a decision waiting in the workspace. Nothing here depends on choosing the Managed lane.

DAYS 1–30 · GOVERN

Put the rules in place

- Approve the AI acceptable-use policy and the human-review rule (steering committee, Oct 10).
- Record the five AI systems in the inventory with owners and data touched.
- Rotate the 410-day privileged credentials; enforce 90-day rotation (POAM.2026.001).
- Enforce MFA for contractor accounts (POAM.2026.003).

DAYS 31–60 · REMEDIATE

Close the high findings

- Close public storage and default-encryption findings in staging and production.
- Turn on audit logging in the two secondary regions.
- Branch protection on the 14 CI/CD repositories.
- Classify training and inference data for use cases 3 and 4; DPIA for contract review.

DAYS 61–90 · PROVE

Make it reportable

- SOC 2 pass rate above 80% on live evidence; schedule the Type II window.
- First quarterly ROAR and GROC board pack from the workspace.
- Publish the trust center with the two certificates and the AI governance summary.
- Decide the lane: self-serve on Assurance Multi, or Managed by 3HUE.

OWNERS

Executive sponsor	Chief Operating Officer
Program	Head of Technology
AI governance	General Counsel
Cloud remediation	Platform engineering lead
Evidence and audit	Compliance manager
3HUE	Named vCISO, weekly cadence through day 90

MEASURES AT DAY 90

- Posture score 80 or above (grade B).
- High findings below 120; zero past 90 days on the POA&M.
- All eight AI governance components in place.
- SOC 2 pass rate above 80%; ISO 27001 above 55%.
- Board pack delivered from the workspace, not from slides.

How the Snapshot was done.

Scope

One business unit (Big Venture Incorporated, Energy) and one AI program (five use cases). Cloud environment: AWS Production, Azure Production, Microsoft 365. Two legal entities in the control baseline. Out of scope: the subsidiary's on-premises environment and the OT network, which were noted for a later Snapshot.

Method

1. **Onboarding (days 1–2).** The Client Vision tenant was created, CloudSignals connected to both cloud accounts, and the first scan run.
2. **Interviews (days 3–6).** Technology, security, legal and operations leadership, one structured session each; business owners for the five AI use cases.
3. **Analysis (days 7–8).** Use-case scoring, governance gap review against the eight components, posture and framework read from the scan, ROAR top risks.
4. **Readout (day 10).** This report, the 90-day plan written into the workspace, and the executive readout with the steering committee.

Evidence

Every figure in this report links to a record in the workspace: the scan of September 19, the finding index, the POA&M and the decisions log. The workspace stays with the client after the Snapshot.

WHAT YOU KEEP

- This report and the 90-day plan.
- Your Client Vision tenant, onboarded, with Signals running.
- The AI use-case map and governance gap register.
- The first ROAR and the control baseline.

NEXT STEP

The plan runs in the workspace whichever lane you choose. If 3HUE takes the seat, the Snapshot fee is credited in full to year one of Managed when you continue within 60 days.

Book the lane call: calendly.com/aramirez-vcio/15min
Or write: aramirez@3hue.net · (954) 738-4454

This sample reproduces the structure and depth of a real Snapshot report using the Big Venture Incorporated demo workspace. Names, figures and dates are illustrative. 3HUE Executive Consulting LLC · 3301 N University Dr #100, Coral Springs, FL 33065 · 3hue.net