SAMPLE BOARD PACK · DEMO DATA

3HUE
Executive Consulting

GROC · EXECUTIVE BRIEFING · Q3 2026

Security posture, quarter in review

One posture score, the risks that moved, the decisions the board owns and the plan for next quarter. Generated from the Client Vision workspace, not from slides, so every number traces to a scan, a register entry or a decision.

Prepared for
Board of Directors, Audit & Risk Committee
Big Venture Incorporated

Prepared by
Named vCISO, 3HUE Executive Consulting
Quarter ended September 30, 2026 · scan of September 19

Sources
ROAR (Risk & Opportunities Assessment Report) · GROC (Governance, Risk, Operations & Compliance) · POA&M · decisions log

Classification
Board confidential. This copy uses the Big Venture Incorporated demo workspace; every figure is sample data.

Posture rose one point to 71. Two decisions need the board.

POSTURE SCORE
71/100
Grade B− · ▲ 1 quarter on quarter

OPEN FINDINGS
629
▼ 25 vs last scan · 0 critical

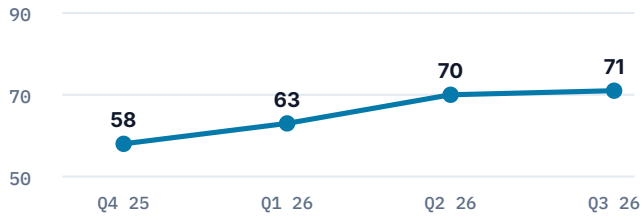
POA&M PAST 90 DAYS
1
▲ 1 · oldest 95 days open

INCIDENTS
0 open
1 declared this year · closed in 6 days

What changed this quarter

- MFA enforced for all 312 employee accounts; contractor accounts remain the gap (POAM.2026.003).
- Daily cloud scanning covers 642 of 662 resources across AWS and Azure; 20 resources in the OT segment are out of scope by decision.
- SOC 2 evidence mapped for 11 of 12 in-scope controls; the Type II window is proposed for Q1.
- The AI governance policy and human-review rule were approved on October 10, ahead of the 90-day plan.
- One deficiency aged past 90 days: privileged credential rotation, blocked on a legacy integration (decision below).

Posture trend · four quarters



DECISIONS FOR THE BOARD

1. **Accept 60 more days on POAM.2026.001** (privileged credential rotation) while the legacy SFTP integration is retired, with compensating monitoring. Recommendation: accept, with a hard stop on December 15.
2. **Renew or retire the standing exception** for the legacy SFTP host, which expires in 30 days. Recommendation: retire; the replacement is in the Q4 plan.

RISK APPETITE · STATUS

Critical findings open	Appetite: 0	WITHIN
POA&M past 90 days	Appetite: 0	BREACHED
Posture score	Target: 80 by Q1	ON TRACK
Exceptions in force	Appetite: ≤ 3	2

Five register risks. Two treatments chosen, one waiting.

ROAR scores each risk on likelihood and impact (1–5), ranked by score then volume. Treatments are decisions recorded in the workspace and mirrored to the finding that raised the risk; the audit trail cannot be rewritten.

#	RISK	SEVERITY	SCORE	TREATMENT	OWNER	STATUS
1	**Privileged cloud credentials without rotation** AWS Production · one set 410 days old	CRITICAL	**20** L4 × I5	Mitigate · rotate and enforce 90-day policy	Platform eng.	PAST 90 DAYS
2	**Publicly reachable storage with sensitive data** Azure Production · 3 containers	HIGH	**16** L4 × I4	Mitigate · private endpoints, access review	Platform eng.	IN PROGRESS
3	**CI/CD repos without branch protection** AWS Production · 14 repositories	HIGH	**16** L4 × I4	Awaiting decision · mitigate or accept for archived repos	Head of Technology	DECISION DUE
4	**Management ports open to the internet** Azure Production · 6 hosts	MEDIUM	**9** L3 × I3	Mitigate · bastion access, close ports	Network lead	IN PROGRESS
5	**Audit logging disabled in secondary regions** AWS Production · 2 regions	MEDIUM	**8** L2 × I4	Mitigate · enable, centralize, 12-month retention	Platform eng.	SCHEDULED

SECURITY EXCEPTIONS IN FORCE · 2

Legacy SFTP host	Expires in 30 days	Board decision 2
Vendor VPN without device posture check	Expires in 74 days	Replacement in Q4 plan

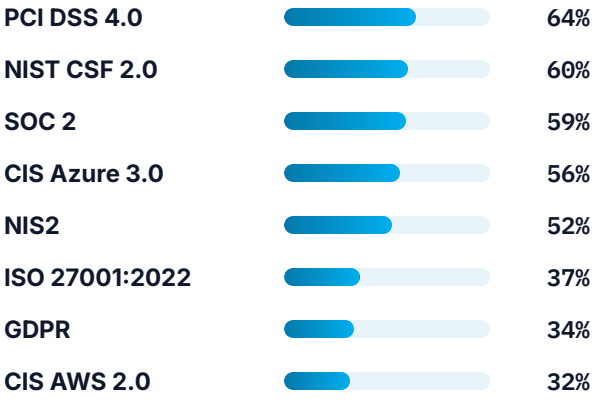
Risk carried knowingly; each exception is reviewed before it expires.

THREAT LANDSCAPE · MONITORED ITEMS

- **CISA KEV:** 3 catalog entries match products in the environment; 2 patched, 1 scheduled (edge appliance, Oct 24).
- **Critical DNSSEC validator flaw** allowing RCE via a malicious zone: not exposed; resolvers are managed.
- **Sector:** two ransomware campaigns against energy operators this quarter; the tabletop on November 6 uses the published playbook.

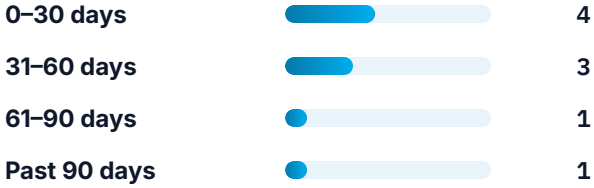
Compliance from the same scan. POA&M aging under control, one exception.

COMPLIANCE SNAPSHOT · PASS RATE · CHANGE VS Q2



SOC 2 up 7 points on the quarter (52% → 59%); ISO 27001 flat pending the ISMS scope decision. Control baseline: 70% implemented, 12 controls governed across 2 entities.

POA&M · 10 TRACKED, 9 OPEN



The 90-day SLA holds for 8 of 9. The one past due is the credential-rotation item in board decision 1. Closed this quarter: POAM.2026.004 (public bucket, Q2).

CERTIFICATIONS AND ATTESTATIONS

SOC 2 Type II	Report dated March 2026; next window proposed Q1 2027
ISO 27001	Certificate valid; surveillance audit April 2027
PCI DSS	SAQ-D self-assessment, on file; 64% automated pass rate
Trust center	Published; 2 certificates, 14 documents, 0 raw findings

Q4: close the high findings, book the SOC 2 window, stand up AI governance.

OCTOBER

Decide and rotate

- Board decisions 1 and 2 recorded; SFTP host retired.
- Privileged credentials rotated; 90-day policy enforced.
- Contractor MFA enforced (POAM.2026.003 closed).
- AI system inventory complete; review rule live in the support copilot.

NOVEMBER

Remediate and rehearse

- Public storage and encryption findings closed in production.
- Audit logging enabled in secondary regions.
- Tabletop exercise, November 6 (ransomware scenario).
- Branch protection decision executed on the 14 repositories.

DECEMBER

Prove

- SOC 2 pass rate above 80% on live evidence; auditor engaged for the Q1 window.
- ISMS scope and Statement of Applicability approved.
- Q4 board pack generated from the workspace.
- Posture target: 78 or above.

INVESTMENT THIS QUARTER

Managed by 3HUE	Seat, RMP and CIRP under the operating plan; no change
Remediation engineering	Forty SEA hours against items 1, 2 and 4
Tooling	None new; Client Vision Assurance Multi, Capacity+ added for the Azure subscriptions
Audit	SOC 2 Type II auditor fees, Q1 budget

HOW TO READ THIS PACK

The posture score is a severity-weighted pass ratio across 2,835 automated checks, the same formula every quarter. Register risks are scored by the risk owner and the vCISO and reviewed monthly. POA&M items carry a 90-day SLA from first observation. Everything on these pages links to a record in the Client Vision workspace; the appendix in the workspace holds the full finding index.

This sample reproduces the structure and depth of a quarterly board pack using the Big Venture Incorporated demo workspace. Names, figures and dates are illustrative. 3HUE Executive Consulting LLC · 3hue.net · (954) 738-4454