GameOps Partner Evaluation · Outsourced Game Operations

How to Evaluate a GameOps Partner

A GameOps partner is not just a vendor watching dashboards. The right partner extends the operating model: monitoring, incident qualification, runbook execution, operational analytics, launch support, recovery validation, and reporting.

IN THIS ARTICLE

- The wrong evaluation criteria
- Can they act, or only notify?
- Do they understand live game operations?
- Can they integrate into your workflows?
- Do they support launch and release windows?
- Do they provide operational analytics?
- How do they handle escalation?
- Questions to ask before choosing a partner

CORE ARGUMENT

Evaluate GameOps partners on their ability to act under pressure.

Many studios and publishers evaluate GameOps support using criteria that look reasonable but do not answer the real question. A partner can have dashboards, a NOC, 24/7 staffing, cloud familiarity, and low pricing — and still be unable to reduce operational risk when players are affected.

The evaluation should focus on whether the partner can move from signal to qualified action, then to verified recovery and operational improvement.

> **A GameOps partner should be evaluated on their ability to act under operational pressure, not just monitor systems or provide coverage.**

WEAK CRITERIA

The wrong evaluation criteria.

These criteria are not useless. They are incomplete. They do not prove that the partner can reduce risk when the game is live.

- “They offer 24/7 monitoring.”
- “They have a NOC.”
- “They support our cloud provider.”
- “They are cheaper than hiring internally.”
- “They have dashboards.”
- “They can escalate to our engineers.”

EVALUATION FRAMEWORK

Seven criteria that actually matter.

The right criteria separate a real GameOps partner from a monitoring vendor, staffing agency, generic NOC, or support outsourcer.

1. Can they act, or only notify?	When an alert fires, what can the partner actually do before escalating? • Approved runbook execution. • Qualified first response. • Access readiness. • Severity and player-impact assessment. • Recovery validation.
2. Do they understand live game operations?	GameOps is not generic IT operations. Live games create player-facing, time-sensitive, operationally specific failure modes. • Launches and CCU spikes. • Matchmaking and authentication issues. • Backend services and API errors. • Payment and entitlement flows. • Latency, packet loss, live events, and player-impact dashboards.

3. Can they integrate into your tools and workflows?	A serious partner should not require a disruptive operating model or force a replacement of the customer's workflow. • Existing-tool integration. • Monitoring and alerting integration. • Slack, Teams, PagerDuty, Jira, or Confluence compatibility. • Runbook alignment. • Customer-owned escalation paths and communication protocols.
4. Do they support launch and release windows?	Launches, patches, hotfixes, live events, and off-hour releases need more than passive monitoring. • Deployment validation support. • Launch-window monitoring. • Hotfix and off-hour release coverage. • Rollback and mitigation decision paths. • Post-release reporting.
5. Do they provide operational analytics, not just monitoring?	Monitoring shows signals. Operational analytics creates context for decision-making, response, and recovery validation. • Dashboards aligned to teams. • Player-impact visibility. • Alert tuning and incident trends. • Executive, producer, engineering, and LiveOps views. • Post-incident reporting and recovery validation.
6. How do they handle escalation?	Escalation should be disciplined, not default. A partner that forwards every alert may increase noise rather than reduce risk. • Known issues handled where safe. • Escalation only when needed. • Defined escalation boundaries. • Fewer unnecessary handoffs. • Protection of internal engineering focus.
7. Is the commercial model aligned with operational reality?	Live-service risk is uneven. The commercial model should not trap the customer in a structure that no longer matches the game's operational needs. • Month-to-month flexibility. • No long-term lock-in. • Ability to scale coverage up or down. • Launch, live event, and legacy-title coverage. • Predictable cost and no unnecessary platform dependency.
The buying test	The strongest question is not "do they monitor?" It is "what changes for our players, internal teams, and business risk when something goes wrong?"

ESCALATION COMPARISON

A strong partner reduces noise. A weak partner adds another handoff.

The easiest way to evaluate a GameOps partner is to inspect what happens after an alert. If the partner cannot qualify, act, validate, or report without immediately routing the issue to your engineers, the model may simply add another layer between signal and resolution.

Strong GameOps partner	Weak GameOps partner
• Handles known issues where safe. • Qualifies player impact and severity. • Executes approved runbooks. • Escalates with context when needed. • Validates recovery and reports outcomes.	• Forwards every alert. • Creates more noise for engineering. • Cannot act without internal teams. • Adds another handoff during incidents. • Leaves recovery validation to the customer.

BUYER CHECKLIST

Questions to ask before choosing a GameOps partner.

These questions force the evaluation away from generic coverage claims and toward operational capability.

- What can you resolve without escalation?
- How do you qualify player impact?
- How do you build, validate, and maintain runbooks?
- What tools do you integrate with?
- How do you validate recovery?
- How do you support launches, patches, hotfixes, and live events?
- What reporting do we receive after incidents?
- What happens after an incident to improve the operating model?
- How quickly can you onboard?
- What is your experience with live online games?

ZUMIDIAN FIT

How Zumidian fits this evaluation model.

Zumidian is built around the idea that outsourced GameOps should extend the customer's operating model, not replace it or add noise. The goal is to help studios and publishers reduce operational risk with qualified coverage, runbook-driven response, operational analytics, and launch support.

The model is most relevant when the customer needs more than alert monitoring: they need a partner that can help turn operational signals into action.

Live-game-specific operations	Built for online games, launches, CCU pressure, live events, backend services, and player-impact risk.
24/7 expert coverage	Around-the-clock operational readiness across incidents, updates, launches, and off-hour windows.
Incident management	Issue qualification, runbook-driven response, escalation coordination, and post-fix verification.
Operational analytics	Dashboards and reporting that support decision-making, response, and recovery validation.
Release and deployment support	Operational coverage for launches, hotfixes, live events, patches, and post-release stabilization.
Ping monitoring	Regional latency and packet-loss visibility for player-impact issues outside core infrastructure metrics.
Existing-tool integration	Operate inside the customer's monitoring, alerting, communication, documentation, and escalation environment.
Flexible commercial model	Month-to-month operating model with no unnecessary long-term lock-in.

BOTTOM LINE

Choose the partner that reduces operational risk, not the vendor with the broadest claim.

A GameOps partner should not be evaluated only by price, monitoring coverage, or the existence of a NOC. Those factors matter, but they are not enough.

The real test is whether the partner can help the game operate better when pressure rises: qualified response, player-impact context, runbook execution, tool integration, launch support, recovery validation, and reporting.

If the partner cannot act, cannot validate recovery, and cannot reduce the burden on internal teams, the business may be buying coverage without readiness.