Vendor Questions Checklist

A structured list of questions your organization can send to a vendor, supplier, or technology partner.

Prepared by: James Kay | UK-based Senior Fullstack Developer & Technical Advisory Consultant

Use: Sample downloadable deliverable for website visitors and advisory prospects. Fictional examples only.

Responsible-use notice: This document is for defensive advisory, vulnerability intelligence, vendor-risk discussion, and remediation planning. It does not include exploit instructions, live-network testing steps, or private vulnerability intelligence.

Purpose

This checklist helps clients ask clear, practical questions when a telecom product, platform, or service may be affected by a vulnerability or advisory.

Questions and Good Answer Guidance

Vendor question	A good answer should clarify
Are we using an affected product or version?	Exact product name, affected versions, fixed versions, and whether the client deployment is included.
Has the issue been fixed in a later release?	Patch, hotfix, maintenance release, fixed version number, release date, and dependencies.
Is there an official advisory, patch, or workaround?	Official reference, patch instructions, workaround steps, and known limitations.
Which interfaces, modules, or deployment modes are affected?	The exact API, management interface, signaling interface, module, or deployment mode.
Is the vulnerable component exposed in our environment?	Whether the interface is internal-only, partner-reachable, internet-reachable, or otherwise restricted.
Can it affect availability, privacy, roaming, fraud, or management operations?	Real-world impact areas and how likely they are in the client deployment.
Are compensating controls available if patching is delayed?	Temporary controls such as access restriction, configuration hardening, firewall rules, or increased monitoring.
What logs or indicators should our team review?	Relevant logs, events, errors, abnormal requests, traffic patterns, or system behavior.
What is the recommended remediation timeline?	Urgency guidance based on severity, exposure, and compensating controls.

Is there a safe way to confirm remediation worked?	Version checks, configuration validation, vendor-approved test method, or log review.

How to Use This Checklist

• Send the relevant questions to the vendor or service provider.

• Record each answer, evidence link, owner, and due date.

• Escalate vague answers that do not provide version, patch, exposure, or timeline details.

• Use the answers to update the internal risk register and remediation plan.

Responsible Boundaries

• No unauthorized testing, scanning, exploitation, or live telecom probing is included.

• Any active assessment, monitoring, or incident response requires separate written authorization and a dedicated scope.

• Private vulnerability intelligence should not be copied, republished, or redistributed outside the applicable license terms.

• This deliverable is intended to support risk understanding, vendor communication, and remediation decisions.