Pelion

Buying the Right SIM:
A Buyer's Guide to IoT Connectivity

Pelion.com

Pelion

Contents

Pelion

1. Introduction

Why IoT Connectivity Procurement Matters

In the rapidly evolving world of the Internet of Things (IoT), selecting the right connectivity partner is not just a technical or sourcing decision, it is a strategic business choice with long-lasting consequences. As IoT deployments scale globally and become more embedded in mission-critical operations, the decisions made during procurement can significantly influence the success, performance, scalability, and security of IoT initiatives for years to come.

Beyond Sourcing: Procurement as a Strategic Enabler

Traditional procurement practices often focus narrowly on price, delivery timelines, and supplier reputation. But IoT connectivity procurement is different. It must account for diverse factors like device lifecycles, regulatory compliance across regions, long-term data costs, roaming capabilities, security standards, SIM management platforms, and evolving connectivity technologies. A poor decision made today, such as locking into an inflexible or regionally constrained provider, can limit future growth and innovation.

This complexity transforms procurement from a tactical function into a strategic enabler of business outcomes. Connectivity affects uptime, customer experience, operational costs, and the ability to enter new markets. The right partner can simplify global expansion, optimize performance, and reduce operational risks, while the wrong one can create costly obstacles down the road.

What is Cellular IoT Connectivity

Among various IoT connectivity options, such as Wi-Fi, LoRaWAN, Bluetooth, and satellite, cellular has emerged as the dominant choice for wide-area, scalable, and mobile use cases, offering secure, reliable coverage at global scale. And with the rise of technologies like LTE-M, NB-IoT, and 5G, cellular is becoming more flexible and energy-efficient, supporting both low-bandwidth sensors and high-bandwidth applications alike.

However, cellular IoT isn't one-size-fits-all. It requires careful consideration of spectrum support, roaming agreements, SIM/eSIM logistics, cost structures, and integration with backend systems. This makes procurement even more critical, as choosing the wrong type of cellular service, or a provider without future-ready capabilities, can undermine the entire IoT business case.

Pelion

The Growth of IoT: Changing Trends Driving Complexity

The IoT landscape is undergoing rapid transformation. New business models, use cases, and deployment geographies are emerging, pushing connectivity needs far beyond what traditional procurement models can handle. As a result, traditional connectivity procurement models are becoming increasingly inadequate as organizations prepare for a future of massive scale, complexity, and long-term commitments.

Trend	2020	2030 (Projected)	Impact on Procurement
Connected Devices[1]	~16B+	30-32B+	Urgent need for massively scalable, cost-efficient global connectivity frameworks
Cellular IoT Share[2]	~13%	16-20%	Cellular adoption increasing; strategic, long-term partnerships with key providers required
Geographic Expansion	NA & EU focus	Truly Global (incl. LATAM, Africa, SEA)	Solutions must support roaming, eSIM/ multi-IMSI, and agile compliance with local laws
Use Cases	Narrowband sensors	Full spectrum: low-power to real-time video	Need for dynamic, application-aware network management and tiered service options
Device Lifecycle	3-5 years	10–15+ years	Procurement must plan for longevity, over-the-air updates, and future-proofing strategies

Connectivity Procurement as a Competitive Advantage

Successful IoT connectivity procurement delivers more than just network access; it becomes a competitive differentiator. Companies that partner with agile, global, and technically advanced connectivity providers are better positioned to:

- Enter new markets faster
- Scale deployments with fewer integration headaches
- Ensure consistent uptime and service levels
- Gain cost predictability across large fleets
- Secure data across borders with regulatory compliance

In short, when done right, connectivity becomes an enabler of innovation, agility, and efficiency, not a constraint. That's why getting procurement right matters now more than ever.

1 - IoT Analytics; 2- Ericsson

Pelion

2. Understanding Business

Needs and Use Cases

Before selecting an IoT connectivity solution, it is critical to develop a clear understanding of your organization's business needs and specific use cases. Connectivity decisions should be guided not just by technical specifications, but by how well they align with broader business goals and operational requirements.

Define the Nature of Your IoT Deployment

Start by assessing whether your IoT devices will be mobile or static. Mobile assets, such as vehicles, delivery equipment, or personnel wearables, will have vastly different connectivity requirements than fixed sensors used in a manufacturing plant or smart building. Mobility often necessitates cellular connectivity for broad geographic coverage, including roaming across networks, whereas static devices might be served by fixed-line, Wi-Fi, or localized LPWAN solutions.

Next, consider data criticality and timing:

- Do you require real-time or near-real-time data?
- Or is periodic batch data transmission sufficient?

This distinction will influence your required bandwidth, latency tolerance, and network reliability. For example, real-time condition monitoring in industrial settings demands low latency and high uptime, whereas soil moisture data for smart agriculture may tolerate longer transmission intervals.

Understand What Data You're Tracking

Clarify whether you are capturing environmental, asset, or behavioral data – or a combination of the three. Each type presents different connectivity and storage challenges.

For example:

- Environmental sensors often need to be deployed in remote or outdoor locations, making long-range, low-power connectivity crucial.
- Behavioral or usage data (e.g., smart home or consumer wearables) typically require more frequent updates and secure handling of sensitive information.

Pelion

Address Vertical-Specific Requirements

Connectivity needs are deeply influenced by industry:

- Smart cities may prioritize interoperability across public infrastructure, seamless handoffs between networks, and massive device scaling.
- Industrial IoT (IIoT) often requires deterministic connectivity, integration with legacy systems, and strong security guarantees.
- Agriculture deployments may span vast rural areas, making multi-network roaming a cost-effective and scalable alternative to single-network MNOs.

Engage Business Units Early

Effective IoT connectivity decisions aren't just IT's responsibility. Engage cross-functional stakeholders early (operations, product, compliance, finance, and end users) to align technical decisions with value delivery and organizational priorities. For instance, the KPIs valued by a logistics team (e.g., asset uptime, route efficiency) may differ from those of IT (e.g., network reliability, cybersecurity compliance).

Understanding the core KPIs and drivers of change (e.g., automation goals, ESG mandates, customer experience improvement) will help prioritize connectivity capabilities that directly support measurable business outcomes.

Plan for Reliability and Scalability

Ensure that your connectivity choices will support not just current needs but future growth.

What to consider:

Scalability

Can your network handle 10,000 devices tomorrow if you start with 1,000 today?

Reliability

What redundancy mechanisms exist? How will devices behave in case of a connectivity failure?

Management at scale

Does your provider support centralized device provisioning, diagnostics, and over-the-air updates?

Using cellular connectivity platforms with built-in failover, automatic carrier switching, or cloud-based management tools can significantly streamline operations and reduce long-term costs.

Pelion

3. Short-Term vs. Long-Term

Deployment Considerations

A successful IoT connectivity strategy must account for both immediate project needs and long-term operational goals. While early-stage efforts like proofs of concept (PoCs), pilots, and minimum viable products (MVPs) allow for experimentation and iteration, production-scale deployments demand robust planning for scalability, automation, and lifecycle longevity. Procurement strategies must bridge this evolution seamlessly.

Short-Term: PoCs, Pilots, and MVPs

In the early stages of IoT deployment, the focus is typically on validating core functionality, testing connectivity under real-world conditions, and refining the user experience.

These short-term projects often involve:

- Localized connectivity (e.g., single region or site-specific deployments).
- Manual or semi-automated provisioning of devices and SIMs.
- Minimal infrastructure for device management or analytics.
- Limited operational and business impact, with tolerance for outages or downtime.

During this phase, procurement teams can prioritize flexibility and speed over scale. Engaging a provider that supports easy onboarding, sandbox environments, and pay-as-you-grow pricing can accelerate testing and reduce risk.

Long-Term: Scaling to Production and Beyond

When transitioning to full production, the requirements expand dramatically. A deployment may involve thousands to millions of devices, each with varying data needs, deployment environments, and connectivity reliability thresholds.

Procurement considerations now include:

- Global coverage across multiple countries and regions.
- Automated provisioning of SIMs and devices, often with zero-touch setup.
- Robust SLAs for uptime, latency, and support.
- End-to-end lifecycle management, including updates, diagnostics, replacements, and deactivation.

Connectivity management platforms (CMPs) must support high-availability architectures and provide centralized management of device fleets. Features like remote SIM provisioning (eSIM or iSIM) and carrier fallback become critical to ensuring seamless performance across regions and over time.

Procurement teams should look for providers that support scalable platforms with open APIs, automated workflows, and the ability to monitor usage, costs, and performance in real time.

Pelion

Planning for the Unknown

A critical consideration, especially in longer-term deployments, is maintaining flexibility in the face of evolving needs. Your data usage may spike as devices collect richer telemetry, integrate AI-driven edge computing, or expand into new business lines. Likewise, your deployment regions may grow beyond initial expectations.

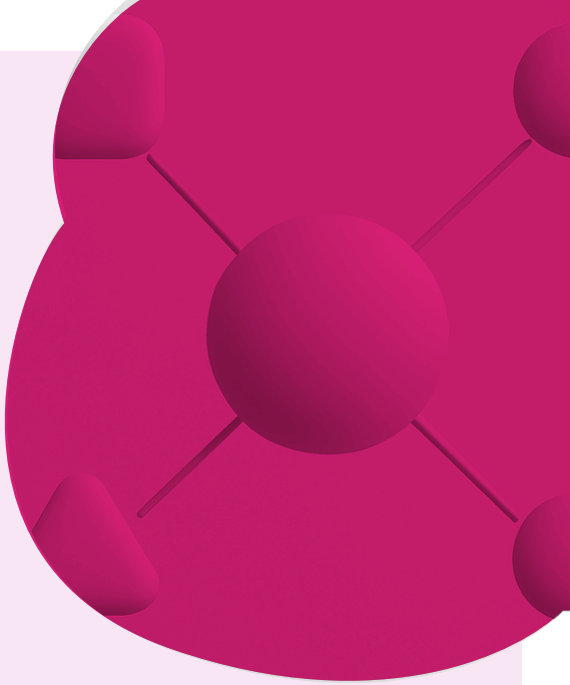
To prepare for these unknowns:

- Consider eUICC-capable embedded SIMs (eSIMs) that allow remote profile switching without physical access.
- Ensure providers can support multi-carrier and cross-border coverage without renegotiating contracts.
- Build in usage forecasting tools and threshold-based alerts to manage cost and performance over time.

Key Takeaways

- Short-term projects validate feasibility;
- long-term deployments demand durability, automation, and foresight.
- Procurement strategies should accommodate both ends of the spectrum, from agile MVP testing to large-scale, mission-critical connectivity, with platforms and partners that support growth, flexibility, and resilience.

Pelion



4. IoT Connectivity

Technology Landscape

Selecting the right IoT connectivity technology is a foundational decision that directly impacts performance, cost, scalability, and coverage. With multiple options available, understanding the strengths, limitations, and ideal use cases of each is essential.

Technology	Best For	Range	Power Use	Data Rate	Cost	Mobility	License Needed
2G/3G	Legacy systems, fallback only	Wide	Medium	Low	Declining	Wide	Licensed
4G LTE	General-purpose, higher data use	Wide	Medium-High	Medium-High	Medium	Wide	Licensed
5G	High bandwidth, ultra-low latency, industrial use	Wide	High	Very High	High	Low	Licensed
LTE-M	Mobile low- power devices (e.g., wearables, logistics)	Wide	Low	Medium	Low-Medium	Medium	Licensed
NB-IoT	Static sensors, deep indoor (e.g., smart meters)	Wide	Very Low	Low	Very Low	Low-Medium	Licensed
LoRaWAN	Rural, remote, low-power static sensors	Long (up to 15km)	Very Low	Low	Very Low	High	Unlicensed (ISM)
Satellite	Remote/off-grid locations (e.g., maritime, mining)	Global	Medium-High	Low-Medium	High	Licensed	Licensed
Wi-Fi	High data rate, local networks	Short (50-100m)	High	High	Low (infra-based)	Licensed	Unlicensed
Bluetooth / BLE	Proximity tracking, wearables, edge sensors	Very Short	Very Low	Low-Medium	Low	Licensed	Unlicensed

Pelion

When to Use What:
Decision Factors

Mobile Assets Across Regions	Use cellular (LTE, LTE-M, 5G) with support for flexibility across carriers and countries.
Static, Remote, Low Data	LoRaWAN or NB-IoT excel in long battery life and cost efficiency.
Industrial Automation or Smart Cities	5G is ideal for low latency and high reliability in dense device environments.
Edge or Localized Environments	Use Wi-Fi or BLE for short-range communication where infrastructure is already available.
No Terrestrial Coverage	Choose satellite for global or off-grid deployments, but factor in higher cost and latency.

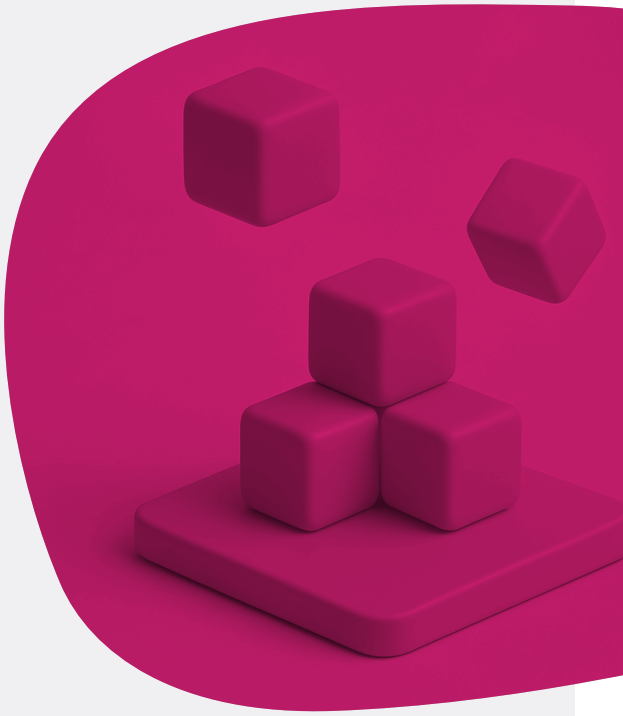
Core Network: Do You Need It?

When choosing an IoT connectivity provider, one key question is whether they operate their own core network or rely on a mobile carrier's infrastructure. The core network is the "brain" of mobile connectivity – it's responsible for authenticating devices, routing data, managing SIM profiles, and enforcing service policies. Some providers invest in running their own core network (either physical or cloud-native), while others resell connectivity from established mobile network operators (MNOs). Both approaches have distinct trade-offs.

Core Network Owned by Provider	Pros	Cons
Yes	• Full control over data routing • Greater flexibility in SIM management • Easier integration with private networks or cloud	• Higher complexity • May require deeper integration work
No (Rely on Carrier Core)	• Faster to deploy • Simpler architecture	• Limited visibility/control • May lack flexibility in roaming or SLAs

For large-scale, mission-critical, or global deployments, working with a supplier who owns their own core network or offers a cloud-native core can improve performance visibility, ensure roaming flexibility, and support future needs like private 5G or network slicing.

Pelion



Infrastructure and Regulatory Considerations

From spectrum licensing and regional coverage variations to cross-border data policies, procurement teams must assess more than just technical fit; they must ensure long-term viability and legal alignment. The regulatory environment can directly affect deployment timelines, device certification, and network availability.

Key considerations that should inform your procurement strategy:

Licensed vs. Unlicensed Spectrum

Cellular and satellite operate in licensed bands and require coordination with regulatory bodies. LoRaWAN, BLE, and Wi-Fi use unlicensed ISM bands, offering easier deployment but with higher interference risk.

Regional Variations

Regulatory frameworks vary by country. For example:

- NB-IoT and LTE-M support is inconsistent across regions.
- LoRaWAN spectrum bands (EU868, US915) differ by region and must comply with local duty cycles.
- Satellite providers may require landing rights or approval for ground terminals.

Partnering with a global IoT MVNO helps navigate these complexities, offering pre-approved roaming agreements, regional fallback options, and built-in compliance. While MNOs offer direct access to national infrastructure, they often lack the cross-border flexibility and unified management platforms provided by MVNOs.

Pelion

Infrastructure and Deployment Considerations

When choosing a connectivity path, consider:

Backhaul requirements	**Does your network need fiber, satellite, or cellular backhaul?**
On-premises vs. cloud	Where will your data terminate? On-site, at a cloud endpoint, or in the provider's infrastructure?
Security & segmentation	Can your network support virtual private networks (VPNs), APNs, or private cores?
Device density & interference	Especially relevant for urban Wi-Fi/BLE or LoRaWAN deployments.

Key Takeaways

- There is no one-size-fits-all IoT connectivity technology. The right choice depends on mobility, power consumption, data needs, region, and scale.
- Consider the long-term cost and operational complexity of managing the chosen network.
- Evaluate whether you need a provider with a dedicated core network for better control and scalability.
- Don't overlook regulatory compliance – partner with vendors who have global connectivity experience and robust legal frameworks.

Pelion

5. Key Connectivity
Provider Selection Criteria

The choice of an IoT connectivity provider is one of the most strategic decisions an organization can make in its deployment journey. Connectivity isn't just about keeping devices online, it's about ensuring operational continuity, scalability, security, and long-term return on investment.

Core Evaluation Areas

1 Coverage & Network Availability

Coverage remains foundational, especially for mobile or geographically distributed deployments. Consider:

- Domestic vs. international reach
- Technology support: 2G/3G (if needed/ available), 4G/LTE, LTE-M, NB-IoT, and 5G
- Network redundancy and multi-carrier fallback support
- Roaming agreements and localized performance

2 Device & SIM Management Capabilities

Scalability and operational efficiency depend on robust SIM lifecycle tools. Look for:

- Real-time SIM status, activation, and diagnostics
- Remote provisioning and bulk onboarding
- Support for eSIM/eUICC and OTA updates
- Policy-based usage controls (data limits, throttling, alerts)

3 Platform APIs & Integration

Modern deployments require tight integration with enterprise systems. Evaluate:

- RESTful APIs for SIM provisioning, device control, and analytics
- Webhook/event support for real-time notifications
- API documentation quality and developer resources
- SDK availability or middleware support

4 Service & Support Models

Support needs grow with complexity and scale. Ensure the provider offers:

- Tiered support with defined SLAs (e.g., <1-hour response for priority issues)
- 24/7 global technical support
- Dedicated account or success managers
- Escalation procedures and transparent incident management

5 Vendor Stability & References

Choose partners positioned for long-term viability. Assess:

- Years in operation, funding, and profitability
- Customer base and active deployments in your industry
- Partnerships with MNOs, MVNOs, and cloud platforms
- Independent reviews, analyst recognition, or certifications

Pelion

Tiered Selection
Criteria Framework

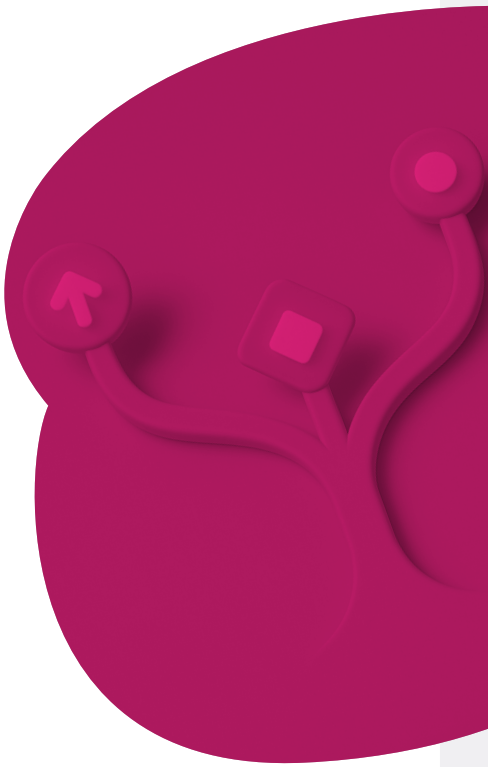
By using a tiered evaluation model, organizations can focus on providers that meet essential operational needs today, while enabling flexibility, performance, and control for future scaling.

Criteria	Must-Have	Nice-to-Have	Deal-Breaker
Coverage	National coverage in all deployment regions	Global roaming, fallback to multiple carriers	No coverage in key markets
SIM Management	Remote activation, real-time status monitoring	eSIM/eUICC support, OTA updates	Manual-only provisioning
API & Integration	Core provisioning and monitoring APIs	Webhooks, developer portal, SDKs	No API access or locked-in platform
Support	24/7 support with basic SLA	Dedicated account manager, knowledge base access	No support SLAs, no escalation path
Vendor Maturity	5+ years in market, operational references available	Industry certifications, enterprise references	No operating history or reference customers
Pricing & Transparency	Predictable pricing model, clear billing	Tiered pricing for bulk or global usage	Hidden fees or usage opacity

Additional Considerations

- **Security & Compliance:** Evaluate providers' security posture (e.g., ISO 27001, SOC 2 compliance) and support for secure data transport.
- **Growth Flexibility:** Can the provider support growth in connected devices without requiring platform changes?
- **Tooling & UX:** Is the provider's console intuitive and built for operations teams?

Pelion



6. Building a Procurement Strategy

A structured procurement strategy ensures that IoT connectivity decisions align with business objectives, technical requirements, and long-term scalability. Given the complexity of IoT deployments, which span connectivity, hardware, platforms, and services, successful procurement demands both rigorous due diligence and agile execution.

Phase 1
Stakeholder Mapping

Stakeholder	Responsibility
IT/Network Engineering	Define connectivity requirements and architecture
Operations / Field Teams	Assess feasibility of deployment, provisioning, and maintenance
Procurement / Legal	Negotiate contracts, manage vendor relationships
Finance	Validate pricing models, budget approvals
Product / Business Units	Ensure connectivity supports business goals and user needs
Security & Compliance	Validate regulatory, privacy, and risk management controls

Phase 2
Technical Requirements Gathering

Before approaching vendors, clearly document both current and future-state needs. This reduces ambiguity in vendor communications and aligns internal expectations.

- Coverage areas (geographic, environmental)
- Network technology preferences (LTE-M, NB-IoT, 5G, satellite, etc.)
- Data throughput and latency requirements
- Device management and provisioning needs
- Security and compliance requirements (e.g., ISO 27001, GDPR)
- Integration needs (API support, cloud compatibility)

Pelion

Phase 3
Route to Purchase

Depending on organizational structure and procurement maturity, different purchase pathways may apply. Understanding your route to market early can influence timelines and RFP structure.

Route to Purchase	Best For
Direct Procurement	Fast-moving teams with technical in-house capacity
Systems Integrators	Complex, multi-vendor deployments
Distributors / Resellers	Standardized solutions or regional support needs
Public Tenders / Portals	Government or highly regulated industries

Phase 4
RFI → RFP → Evaluation → Contracting

Once internal requirements are clearly defined and stakeholder alignment is established, the formal procurement cycle begins. This phase is designed to reduce risk, validate market fit, and ensure that selected vendors can meet both technical and commercial expectations at scale.

Each stage plays a distinct role in narrowing the field and confirming vendor suitability:

Stage	Purpose
RFI (Request for Information)	Broad market scan to identify capable suppliers
RFP (Request for Proposal)	Detailed request outlining technical and commercial requirements
Evaluation	Scorecard-driven assessment of vendor responses, demos, and references
Contracting	Final negotiation of SLAs, pricing, terms, and compliance frameworks

Consider using weighted evaluation frameworks to balance technical, commercial, and operational criteria. For example:

Evaluation Criteria	Weight
Technical Fit (coverage, APIs)	30%
Cost & Pricing Model	25%
Service & Support Model	20%
Flexibility & Scalability	15%
Vendor Stability & References	10%

Balancing Due Diligence with Agile Execution

Procurement teams must balance the need for comprehensive due diligence with the urgency of time-to-market. Key tactics to enable agility while maintaining control:

- Use pilot phases or limited-scope contracts before full rollout.
- Prioritize must-have features early in RFPs to reduce decision cycles.
- Maintain cross-functional alignment through recurring check-ins during evaluation.
- Establish clear go/no-go criteria at each stage of the process.

7. Evaluating Vendors
Test, Pilot, Compare

Even the most thorough procurement process cannot substitute for real-world validation. A structured evaluation phase reduces risk, exposes operational limitations, and ensures that selected vendors meet technical and business expectations.

Establish Pilot Objectives and KPIs

Before initiating a test or pilot, clearly define what success looks like. Key areas to evaluate include:

KPI Category	Sample Metrics
Network Performance	Latency (ms), uptime (%), packet loss (%)
Provisioning & Management	Time to provision SIM/device, ease of API integration, remote
Coverage Reliability	Connectivity stability across regions, handover between networks
Multi-Network Behavior	Fallback response time, SIM switching effectiveness
Support Responsiveness	Time to first response, resolution time, quality of documentation
Integration Depth	API coverage, webhook support, platform compatibility (cloud, MDM)
Battery & Data Usage	Data usage per cycle, impact on device battery life

Pelion

Best Practices for Vendor Trials

1 Use representative devices and environments

Ensure test results reflect the realities of deployment. Include:

- A mix of intended production devices (sensors, gateways, trackers, etc.)
- Representative environments (urban/rural, indoor/outdoor, static/mobile)
- Expected power conditions and installation configurations

2 Test multi-network and fallback capabilities

If using multi-network SIMs or providers promising redundancy, verify:

- Automatic fallback behavior during coverage loss
- Roaming performance and reconnection times
- Network selection logic (manual, automatic, policy-driven)

3 Validate provisioning and lifecycle management

Assess how intuitive and efficient the management platform is. This includes:

- SIM ordering and activation process
- Dashboard usability
- API integration into your provisioning workflows

4 Confirm support & onboarding quality

A good vendor offers hands-on support during the pilot. Evaluate:

- Availability of a dedicated technical contact
- Quality of documentation and onboarding materials
- Responsiveness to questions and issues

Defining Success Criteria

Establish a formal evaluation framework in advance and share these success criteria with vendors to establish a shared understanding of goals and expectations.

Example:

Success Factor	Threshold for Acceptance
Uptime	≥ 99.995% during testing period
Average Latency	≤ 200ms (or project-specific baseline)
Provisioning Time	≤ 5 minutes per device via API
Support Response Time	≤ 2 hours for Tier 1 issues
Integration Time	≤ 3 days to complete API integration
Fallback Test Success Rate	≥ 95% successful network switches

Pelion

8. Scoring Matrix for Vendor Selection

Selecting the right IoT connectivity provider involves multiple dimensions: technical capabilities, commercial terms, operational fit, and long-term vision. A scoring matrix allows organizations to evaluate vendors systematically, apply consistent criteria, and ensure alignment with project priorities.

Vendor Scoring Matrix (Sample Template)

Criteria	Weight (%)	Vendor A Score (1–5)	Vendor B Score (1–5)	Vendor C Score (1–5)	Vendor A Weighted	Vendor B Weighted	Vendor C Weighted
Network Coverage & Tech Options	20	4	5	3	0.80	1.00	0.60
Security & Compliance	15	5	4	4	0.75	0.60	0.60
Pricing & Flexibility	15	3	4	5	0.45	0.60	0.75
SIM Lifecycle Management	10	4	5	4	0.40	0.50	0.40
API & Platform Integration	15	5	3	4	0.75	0.45	0.60
Support & SLAs	10	4	4	5	0.40	0.40	0.50
Innovation / Future Readiness	10	4	4	3	0.40	0.40	0.30
References & Reputation	5	5	3	4	0.25	0.15	0.20
Total Weighted Score	100				4.20	4.10	3.95

This downloadable and editable Excel version of this scoring matrix is recommended to:

- Add/remove vendors
- Modify weights and scoring scales
- Auto-calculate total scores using embedded formulas
- Include notes or qualitative assessments alongside numerical scores

Pelion

9. Cost Models
and Commercial Flexibility

Selecting the right commercial structure can significantly influence the total cost of ownership (TCO), predictability of spend, and the ability to scale efficiently.

Pricing Model	Description	Best Suited For	Risks/Trade-offs
Per-device flat rates	Fixed monthly fee per SIM/ device, regardless of usage.	Predictable, low-data-use devices; MVPs and pilots	May result in overpayment for low-usage devices
Pooled/shared bundles	Shared data allowance across all devices in a fleet.	Fleets with mixed usage patterns	Risk of overage if pool sizing is poor
Pay-as-you-go	Charged strictly based on actual data consumed.	Variable or seasonal traffic patterns	Unpredictable billing; can spike unexpectedly
Reserved capacity	Committed monthly data usage at discounted rate (w/penalties for underuse).	Large-scale, predictable deployments	Lack of flexibility; underutilization costs

Key Commercial Flexibility Levers

Beyond core pricing models, flexibility in contract terms is vital to reducing risk and enabling scalability.

1 Break clauses

- Allow early termination of contracts without full penalties.
- Useful for PoCs or evolving tech environments where future requirements are uncertain.

2 Volume discounts

- Tiered pricing models based on number of SIMs or GB/month can unlock significant savings.
- Important to negotiate clear thresholds and ensure they align with projected growth.

3 Overage policies

- Define how additional usage beyond the plan is billed – by MB/GB and at what rate.
- Transparent and capped overage fees reduce financial surprises.

4 Bundled services

- Many providers offer bundles including:
  - SIMs + platform access
  - SIMs + hardware
  - Global roaming + management APIs
- Bundling can simplify procurement and offer price advantages but should be weighed against potential vendor lock-in.

Pelion

Sample Cost
Impact Comparison (Per SIM/Month)

Usage Scenario	Flat Rate	Pooled Plan	Pay-as-you-go
Static sensor (50MB/month)	$1.50	$1.20	$0.80
Mobile asset tracker (250MB)	$1.50	$1.00	$2.00
Video feed device (1GB)	$1.50	$1.50	$5.00

Note: Actual rates will vary by geography and vendor. This table is illustrative.

Strategic Considerations:

- **Total cost vs. predictability:** Decide whether financial predictability or efficiency at scale is the higher priority.
- **Contract duration vs. flexibility:** Longer-term commitments can unlock better pricing but may limit agility.
- **Scalability of the model:** Ensure pricing models do not penalize growth or require full renegotiation when scaling from 100s to 100,000s of devices.

Procurement Tip

Ensure that commercial flexibility is scored as part of your evaluation framework. Use scenarios to test how different models behave under scaling, regional expansion, and failure conditions.

Pelion

10. Security, Compliance
& Risk Management

In IoT deployments, security is not just a checkbox; it's an ongoing discipline. Vendors should demonstrate both current credentials and a roadmap for continued improvement, including incident response protocols, audit trails, and compliance reporting features.

If you're operating in regulated industries (e.g., healthcare, finance, government), work with legal and compliance teams early in the procurement cycle to validate all obligations.

Core Areas of IoT Connectivity Security

Security Domain	What to Assess	Why It Matters
Data in Transit	End-to-end encryption (e.g., TLS, IPsec), private APNs, VPN tunneling	Prevents interception or tampering during communication
Data at Rest	Storage encryption, access control on backend platforms and dashboards	Protects sensitive telemetry and user data when stored
Device Identity & Authorization	Unique identifiers, secure boot, mutual authentication (e.g., certificates or pre-shared keys)	Ensures only authorized devices connect to the network
SIM Security	eSIM/eUICC capabilities, SIM locking, profile management	Reduces risk of SIM fraud and supports secure over-the-air provisioning
SIM Security	Token-based access, rate limiting, audit logs, role-based permissions	Secures integration points with your systems

Pelion

Compliance & Regulatory Requirements

Framework / Regulation	Focus Area	Relevance to IoT
GDPR (EU)	Personal data protection	Ensures IoT data containing user or location info is handled lawfully
UK Data Protection Act	UK-specific implementation of GDPR	Critical for UK-based operations or cross-border data transfers
Data Residency Laws	Jurisdictional storage/processing	Some countries require data to be stored locally (e.g., India, Brazil, China)
ISO 27001	Information security management system (ISMS)	Indicates mature organizational security practices
Cyber Essentials	UK government-backed security certification	Baseline for organizational cybersecurity controls
Industry-specific	HIPAA (Healthcare), PCI-DSS (Payments), etc.	Applies to verticals with specialized compliance obligations

Questions to ask vendors:

1. **How is IoT data encrypted at rest and in transit?**
2. **Do you offer secure provisioning via eUICC or eSIM remote profile management?**
3. **Can you provide a list of current security certifications (e.g., ISO 27001)?**
4. **Do you maintain full compliance with regional data residency laws for all operating regions?**
5. **How are user roles, permissions, and access managed on your management platform?**
6. **Is penetration testing conducted regularly? By whom?**

Security Risk Assessment Checklist

Risk Area	Mitigation Strategy	Vendor Capability Required
Device spoofing	Mutual authentication, unique identifiers	Secure device provisioning and credential management
Network sniffing	Encrypted tunnels (VPN, TLS), private APNs	End-to-end encrypted data paths
SIM fraud	SIM locking, IMEI whitelisting, eSIM with profile control	Advanced SIM lifecycle management tools
Data exfiltration from APIs	API key rotation, RBAC, rate limiting	Secure, auditable API access with usage controls
Unauthorized platform access	SSO integration, MFA support	Enterprise-grade identity & access management on web portal

Pelion

11. Managing Scale:

SIM Management, Roaming & Global Reach

As IoT deployments grow, managing connectivity at scale calls for smarter solutions. By moving beyond manual provisioning and local setups, enterprises benefit from scalable SIM management and global strategies, while also keeping control.

This table covers advanced SIM technologies, global roaming strategies, centralized management tools, and policy controls, each critical for ensuring seamless, secure, and cost-efficient operations across vast networks.

Key Concepts for Scalable Connectivity

Capability	Description	Why It Matters
Global or Multi-IMSI SIMs	SIMs with multiple network profiles or IMSIs embedded	Provides seamless roaming across regions without swapping SIMs
eUICC (Embedded SIMs)	Remote provisioning of SIM profiles over the air (OTA)	Future-proofs deployments and reduces vendor lock-in
Roaming Agreements	Pre-negotiated global roaming across networks	Critical for cross-border or international asset tracking
Connectivity Management Portals	Centralized interface for managing thousands of SIMs	Enables automation, visibility, and real-time policy enforcement
Policy Enforcement	Rules for data usage, location restrictions, usage caps	Prevents misuse, fraud, or unexpected costs

Pelion

Best Practices for SIM & Deployment Management at Scale

1 Adopt a centralized SIM management portal

- Look for platforms that support bulk activation/deactivation, tagging, grouping, and analytics.
- Integration via API is key for automated provisioning at the manufacturing stage.

2 Implement remote SIM provisioning

- Ensure support for eUICC (GSMA-compliant) and remote profile management to reduce logistics costs.
- Remote provisioning reduces the need to physically access devices to change operators.

3 Use multi-IMSI or global SIMs

- For mobile assets and global fleets, ensure SIMs can connect to multiple local networks.
- Prioritize solutions that offer steered and non-steered roaming options depending on your needs.

4 Monitor & manage churn

- Establish policies to identify inactive SIMs.
- Consider automated suspension after periods of inactivity to reduce unnecessary charges.

5 Secure lost or stolen SIMs

- Require the ability to remotely lock, deactivate, or blacklist SIMs instantly.
- Use IMEI locking to restrict SIM usage to known devices.

6 Apply usage policies proactively

- Enforce data limits, block usage in unauthorized regions, and set up alerts for abnormal traffic.
- Automatically shift high-usage devices to pooled plans or higher tiers to control costs.

Pelion

Features to look for Fleet' to Connectivity so it reads: Features to look for in a Connectivity Management Platform

- Bulk SIM provisioning
- Role-based access control (RBAC)
- Real-time diagnostics & status
- Automated alerts (usage, roaming)
- API integration with backend systems
- Profile switching (multi-IMSI/eUICC)

Tips for Global Deployments

Test in each target market:

Not all SIMs perform equally in all countries due to roaming restrictions, latency, or limited partner networks.

Ensure legal compliance:

Roaming is not permitted in some countries for permanent IoT installations (e.g., Turkey, India). Work with vendors that offer local breakout or permanent roaming solutions.

Plan for future scale:

Choose providers with proven deployments in high-scale scenarios (e.g., over 1M SIMs) and distributed support operations.

Pelion

12. Procurement Process Flow:

From RFP to Contract

Procuring IoT connectivity involves more than choosing a vendor, it requires a clear, structured process to align technical needs, budget, and long-term goals, allowing organizations make informed decisions, minimize risk, and secure the right connectivity partner.

Overview of the Procurement Journey

	Stage	Key Activities	Deliverables/Tools
1	**Preparation**	Define requirements, assess market, draft RFI/RFP	RFI/RFP Templates, NDA templates
2	**Solicitation**	Issue RFP, manage vendor questions	RFP issuance, Vendor Q&A management
3	**Evaluation**	Assess vendor proposals using scorecards	Vendor Scorecards
4	**Negotiation**	Negotiate pricing, service levels, support terms	Contract negotiation levers
5	**Contracting**	Finalize contract including change requests and exit clauses	Signed contract, Change Request Terms, Exit Clauses
6	**Post-Contract**	Monitor performance and compliance	Vendor scorecard updates, SLA monitoring

Pelion

Preparation:
RFI/RFP and NDA Management

Use standardized templates to clearly articulate requirements, evaluation criteria, and timelines to ensure consistency and completeness across procurement activities.

Element	Description
Purpose	Clearly state the objective of the RFI/RFP and the scope of the connectivity need.
Requirements	Define technical, functional, and operational requirements in detail.
Evaluation Criteria	Outline how proposals will be assessed (e.g., cost, coverage, scalability).
Vendor Information	Request relevant experience, certifications, references, and capabilities.
Timeline	Include key dates for submission, review, and decision-making.
Submission Guidelines	Provide instructions on format, delivery method, and point of contact.

Non-Disclosure Agreements (NDAs)

Before vendors can provide technical documentation, coverage maps, SIM provisioning models, or custom pricing, both parties must be protected by a mutual understanding of confidentiality, ensuring that proprietary information shared during the RFI/RFP, pilot, or negotiation phases remains secure and legally protected.

Pelion

Best practices for NDA management:

Initiate early	Begin NDA discussions during or immediately after market engagement, before any technical or pricing disclosures.
Use a standard template	Provide your legal-approved NDA to streamline the process; review vendor redlines.
Make it mutual	Ensure the NDA protects both your organization and the vendor, especially if you're sharing internal architecture or pilot results.
Track signatures	Maintain a centralized record of which vendors have executed NDAs and the dates of signing to avoid compliance gaps during evaluation.
Align with procurement timelines	NDAs should be signed before distributing RFPs or technical specifications to maintain control over sensitive materials.

Evaluation:
Vendor Scorecards

Develop scorecards tailored to your key criteria such as price, compliance, technical capability, and support. Assign weights to each criterion based on organizational priorities. Use scorecards to drive transparent and objective evaluations. Example:

Evaluation Criterion	Weight (%)	Notes
Price	30	Total cost of ownership
Service Level Agreements	25	Response and resolution times
Support & Maintenance	20	Availability and quality of support
Technical Compliance	15	Alignment with technical specs
Vendor Reputations	10	Past performance and references

Negotiation:
Leveraging Contract Terms

The negotiation phase is a critical opportunity to shape the long-term value and performance of the partnership. Beyond pricing alone, negotiation should also cover service expectations, operational support, and financial flexibility.

Negotiation Lever	Focus Area	Typical Approaches
Price	Total cost, payment terms	Volume discounts, milestone payments
Service Level Agreements (SLAs)	Response time, uptime, penalties	Define measurable KPIs, penalty clauses
Support	Helpdesk availability, escalation procedures	24/7 support, dedicated account manager

Pelion

Contracting:
Incorporating Critical Terms

Two often overlooked but critical components of the contract are Change Request Terms and Exit Clauses. These protect both parties by providing structured pathways to adapt or disengage, without creating operational disruption or legal ambiguity.

Change Request Terms

In IoT deployments, change is inevitable. Shifts in device volume, geographic reach, data usage patterns, or regulatory requirements can all impact connectivity needs. Change Request Terms in the contract should anticipate these dynamics and offer a controlled mechanism for adapting the scope of services without renegotiating the entire agreement.

Key Considerations

- **Defined Scope Change Process:** Include a formal process for submitting, reviewing, and approving change requests—covering both commercial and technical modifications.
- **Approval Governance:** Specify which stakeholders (from both buyer and provider sides) are authorized to approve changes, and under what conditions.
- **Impact Assessment Requirements:** Require the vendor to provide cost, timeline, and performance impact assessments for any proposed changes before approval.
- **Examples of Scope Changes:** Adding/removing SIMs, activating new regions, upgrading to eSIMs or 5G RedCap, integrating new APIs, or adjusting data usage plans.

Why It matters

IoT connectivity contracts that don't allow for structured changes risk becoming obsolete quickly, leading to shadow contracts, misaligned expectations, or cost overruns.

Pelion

Exit Clauses

While partnerships are entered into with the best intentions, IoT connectivity buyers must protect against underperformance, misalignment, or changes in strategic direction. Exit Clauses provide a legal and operational framework for disengaging from a provider with minimal disruption to services, compliance, and customer experience.

Key Considerations

- **Notice Periods:** Define realistic notice periods for both termination for cause (e.g., SLA breach, security failure) and termination for convenience.
- **Exit Triggers:** Include specific conditions that permit termination without penalty, such as vendor insolvency, merger/acquisition conflicts, or failure to deliver key services.
- **Handover & Transition Requirements:** Require vendors to cooperate during offboarding, including SIM deactivation, data transfer, and technical documentation handover.
- **Penalty & Refund Terms:** Clearly state any early termination penalties, refund provisions, or service credits owed upon exit.
- **Survivability of Terms:** Identify which terms (e.g., confidentiality, data protection) remain in effect after termination.

Why It matters

IoT deployments may span multiple years and geographies. A well-crafted exit strategy ensures continuity, protects critical infrastructure, and prevents vendor lock-in.

Procurement Process Flow: From RFP to Contract

Pelion

13. Common Pitfalls and How to Avoid Them

Because IoT solutions typically include a mix of devices, connectivity, data platforms, APIs, and long-term service commitments, buyers must navigate unique challenges that go far beyond traditional software while also evaluating more than just features and price.

Here are common procurement pitfalls specific to IoT, with strategies to help buyers make informed, future-ready decisions.

Vendor lock-in via closed platforms or proprietary APIs

The Challenge

Proprietary APIs or closed ecosystems make it difficult to migrate data, switch providers, or integrate with third-party systems, which can result in long-term dependency and reduced flexibility.

How to avoid it

- Prioritize open standards and interoperability in your RFP.
- Demand access to API documentation and test integration feasibility before committing.
- Include data portability clauses in the contract (e.g., data must be exportable in non-proprietary formats on demand).

Vendor Lock-In Red Flags

Red Flag	What to Ask or Require
Only proprietary protocols supported	Do you support MQTT, CoAP, HTTPS, or LwM2M?
No API documentation upfront	Provide API docs and sandbox access with proposal.
Restrictions on data export	Include a clause ensuring full data access rights.

Pelion

Underestimating
Long-term costs

The Challenge

Connectivity is the backbone of any IoT deployment – and one of its most persistent operating costs. Buyers who evaluate connectivity through a multi-year, lifecycle-oriented lens are far better positioned to manage costs, optimize performance, and avoid post-contract surprises. Without careful consideration of ongoing SIM management, roaming complexity, platform fees, overage charges, and support costs, organizations risk significant budget overruns as deployments scale beyond the pilot phase.

How to avoid it

- Request a Total Cost of Ownership (TCO) breakdown over a 3–5-year horizon. Ensure this includes data, support, SIM management, and any platform or dashboard subscriptions.
- **Include SIM lifecycle services in your procurement requirements:** provisioning, diagnostics, remote suspension/resumption, and replacement costs.
- **Clarify pricing models:** Determine if costs are calculated per device, per MB, per event, or based on time-based tiers. Ask what happens when thresholds are exceeded and whether throttling or overage penalties apply.
- Ask about roaming policies and rates, especially if your deployment spans multiple regions or is mobile in nature (e.g. logistics, smart agriculture, or transportation).

To surface hidden costs and differentiate vendors, ask the following questions:

Category	Question
Pricing Model	Is pricing based on usage (MB), device count, time period, or event-based?
Overage Charges	What are the charges if monthly data caps are exceeded?
SIM Lifecycle	Are provisioning, activation, suspension, and replacement included?
Roaming Policy	What countries are covered? Are there roaming surcharges or zones?
Platform Access	Is portal access included? Are alerts, reports, and APIs chargeable?
Data Pooling	Can data be pooled across devices or regions? What pooling model is used?
Contract Flexibility	Can SIMs be paused or reassigned without penalties?

Pro tip

Don't just ask how much the SIM costs per month. Ask what it will cost to run, manage, and scale connectivity across your full IoT footprint for the next 3 to 5 years.

Pelion

Missing
Integration Complexities

The Challenge

IoT solutions often need to integrate with existing systems like ERP, CRM, supply chain, analytics, or security infrastructure. Poor integration planning leads to siloed data, manual workarounds, and operational friction.

How to avoid it

- Ask for real-world integration examples with your existing systems.
- Include an integration architecture section in your RFP.
- Clarify whether the vendor supports middleware platforms.

Evaluation Tip

To surface hidden costs and differentiate vendors, ask the following questions:

Integration Criterion	Weight	Notes
ERP/CRM Integration	20%	Pre-built connectors or custom work?
API Flexibility	25%	RESTful, secure, well-documented APIs
Edge-to-Cloud Integration	15%	Can local devices push to cloud?
Data Pipeline Compatibility	15%	Kafka, MQTT, AWS Kinesis, etc.
Security/Identity Sync	25%	OAuth, LDAP, or token-based?

Choosing Tech
That Doesn't Scale Internationally

The Challenge

Many IoT buyers deploy solutions regionally, only to find later that scaling globally introduces unforeseen obstacles such as compliance with data laws, hardware certification, roaming restrictions, or lack of local support.

How to avoid it

- Evaluate regulatory compatibility in every market you plan to operate (e.g., GDPR, CE, FCC, PTCRB).
- Confirm whether your IoT devices are pre-certified for global deployment.
- Choose platforms with multi-region cloud support and global SIM provisioning capabilities.

Global Readiness Checklist

Area	What to Validate
Device Certifications	UKCA (UK), CE (EU), FCC (US), IC (Canada), others?
Regional Cloud Support	AWS/Azure/GCP regions aligned with deployments?
Roaming Agreements	Do SIMs work seamlessly across countries?
Data Compliance	Are vendor platforms GDPR/ CCPA compliant?
Language/Localization	Multi-language UI and dashboards available?

Be Proactive, Not Reactive

By incorporating questions and requirements that address lock-in, long-term costs, integration realities, and global scale, buyers can make strategic, future-proof decisions.

Above all, treat IoT procurement as a long-term lifecycle partnership, not just a transactional vendor choice. The right diligence today avoids expensive regrets tomorrow.

Pelion

14. Futureproofing:

Preparing for Tech and Market Change

IoT ecosystems are evolving rapidly, driven by changes in network standards (e.g., 5G RedCap, LPWAN), new provisioning models (eSIM, iSIM), and emerging hybrid connectivity methods (e.g., cellular-satellite). Buyers who fail to consider how today's procurement decisions will perform under tomorrow's conditions risk being locked into obsolete infrastructure, stranded assets, or providers that can't scale.

Build abstraction layers for portability

Why it matters

Tightly coupled systems, where devices, SIMs, platforms, and analytics are all managed by a single vendor, can be convenient at first but make it harder to switch vendors or evolve architectures later. Abstraction layers can decouple these components, allowing greater flexibility and migration capability over time.

What to do

- Use middleware platforms or connectivity management layers that support multiple carriers or protocols.
- Select vendor-neutral device management platforms that can manage devices across networks and hardware types.
- Ensure your solution includes standard APIs and does not rely on proprietary formats for critical data or control functions.

Key considerations

Component	Recommendation
Device Management	Use platforms that support multiple connectivity types
SIM Control Layer	Prefer providers that expose full SIM management via API
Cloud Integration	Ensure cloud APIs (for AWS, Azure, etc.) are modular and portable
Analytics/BI Tools	Decouple data pipeline from hardware or connectivity providers

Pelion

Select providers
who evolve with the market

Why it matters

Many providers specialize in today's dominant technology (e.g., LTE-M or NB-IoT) but may not offer clear roadmaps for next-generation tech like 5G RedCap or satellite fallback. Your provider should demonstrate long-term investment in innovation and an ability to evolve with market and regulatory demands.

What to look for

- Providers offering eSIM or iSIM support, allowing remote profile switching and device provisioning.
- Roadmaps that include 5G RedCap, a lightweight 5G variant ideal for mid-complexity IoT use cases (e.g., wearables, industrial sensors).
- Hybrid connectivity options that combine terrestrial (cellular) and satellite coverage for global or remote deployments.
- Evidence of frequent platform upgrades, SDK updates, and standards alignment (e.g., GSMA, 3GPP).

Checklist: Future-Ready connectivity providers

Feature	Ideal Capability
eSIM/iSIM Support	Yes, including remote SIM provisioning (RSP)
5G RedCap Roadmap	Confirm deployment dates and coverage roadmap
Satellite Integration	Partnered or native hybrid offerings (e.g., LTE + LEO)
Update Cycle Transparency	Release notes, update cadence, support documentation

Ensure devices support
OTA updates for long-term viability

Why it matters

IoT devices may be deployed for 5–10 years or even more. The ability to push firmware updates over the air (OTA) is essential for maintaining security, compliance, and feature parity over time. Without OTA capability, fleets of devices risk becoming outdated or vulnerable.

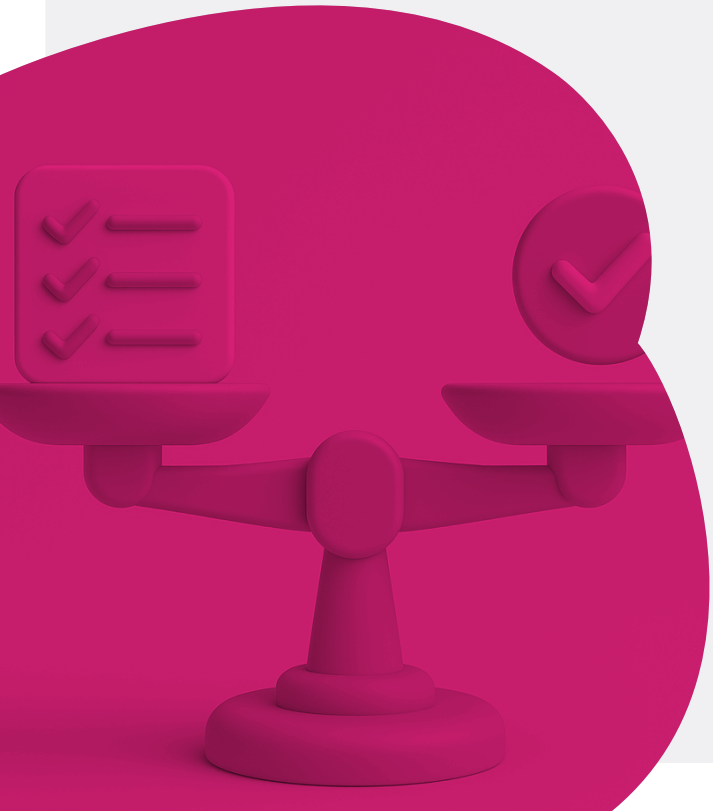
What to require

- Explicit support for OTA firmware updates as part of your device and connectivity stack.
- Secure mechanisms for authentication and rollback in the case of failed updates.
- Support for differential updates (only pushing changes, not full firmware) to reduce bandwidth and cost.

OTA evaluation criteria

OTA Feature	Best Practice
Update Triggering	Manual and automated update scheduling supported
Secure Delivery	Encrypted, signed firmware packages
Rollback Mechanism	Devices can revert to last known good firmware
Bandwidth Efficiency	Differential or compressed updates available
Vendor Role	Clarify whether OTA is vendor- or customer-managed

Futureproofing is not about predicting the next trend perfectly, it's about designing flexibility into your procurement decisions. By choosing modular, open, and evolvable components across connectivity, hardware, and software, buyers can adapt as networks evolve, standards change, and global market conditions shift.



Pelion

15. Conclusion:

Procurement as a Strategic Lever in the IoT Journey

Connectivity isn't just a technical decision, it's a strategic one. As organizations race to unlock the full potential of the Internet of Things, the choices made in procurement will define whether IoT becomes a scalable engine of value or an uncontrolled cost center.

It all starts with business goals. Too many initiatives begin with devices and networks, but the smartest buyers flip the script. They start by asking: ***What outcomes are we driving? Who benefits and how do we measure success?*** Only then do they align connectivity to value delivery across operations, customer experience, and strategic growth.

From there, success requires designing for scale. That means choosing platforms and partners that support global reach, automated SIM lifecycle management, and visibility from deployment to retirement. It's not enough to connect a few thousand devices. The real challenge is managing millions efficiently, securely, and predictably.

Still, scale shouldn't come at the cost of flexibility. Striking a balance is crucial: piloting quickly to learn but evaluating rigorously before expanding. Integration complexity, support responsiveness, and total cost of ownership often surface only after launch, making early diligence essential.

This is also where future-proofing matters. IoT is quickly evolving, and procurement choices made today must accommodate tomorrow's innovations. Short-term savings often lead to long-term limitations. Wise buyers avoid that trap by choosing architectures and vendors built for longevity.

Finally, success in IoT isn't just about technology, it's about people and process. Connectivity touches every part of the business, from operations and IT to finance, compliance, and cybersecurity. Procurement leaders who engage these stakeholders early build alignment, reduce friction, and ensure smoother, more sustainable rollouts.

In the end, connectivity is one of the most persistent and impactful elements of any IoT deployment. Treat it not as a line item, but as a long-term investment. Buyers who think strategically across lifecycle, scale, flexibility, and cross-functional collaboration don't just avoid surprises – they unlock the full power of IoT.

Pelion

Internal
Alignment Checklist

Use this checklist to prepare your organization before engaging the market. Cross-functional clarity now will prevent downstream delays and misalignment.

Area	Key Questions
Business Readiness	What problem are we solving? What use case is the highest priority to launch?
Budget and Ownership	What's the projected 3–5 year spend? Who owns ongoing SIM and platform costs?
Security & Compliance	What internal or regulatory standards must our provider meet?
Integration Strategy	What systems must the connectivity platform integrate with (e.g., ERP, analytics)?
Procurement Model	Are we going direct, through partners, or via framework agreements?
Pilot Goals	How will success be measured during trials (e.g., uptime, ease of provisioning)?

90-Day Roadmap:
From Planning to Vendor Decision

The following example roadmap offers a time-bound framework for moving from internal planning to vendor selection.

	Phase	Weeks	Key Milestones
1	**Discovery & Planning**	Weeks 1–3	• Finalize use case(s) and business goals • Align stakeholders & budget
2	**Market Engagement**	Weeks 4–6	• Issue RFI or conduct early market scans • Identify longlist of suitable providers
3	**Pilot Design**	Weeks 7–9	• Define pilot parameters, devices, success metrics • Engage shortlisted vendors
4	**Pilot Execution**	Weeks 10–12	• Run test deployments • Evaluate network performance, support, portal, APIs
5	**Vendor Selection**	End Week 12	• Score vendors using defined matrix • Begin contract negotiation

Pelion

Closing Thoughts

In an IoT environment where technologies, standards, and business needs evolve rapidly, procurement must be as agile as it is rigorous. The best decisions will balance today's operational priorities with tomorrow's uncertainties, selecting partners, platforms, and technologies that offer not just performance, but resilience and adaptability.

This guide is your starting point. The next step is yours.

Cellular IoT Connectivity Procurement Checklist

Use this checklist to evaluate providers.

1 Coverage & Network Access

- ☐ Is global, regional, or national coverage available as needed?
- ☐ Are all required radio access technologies supported (2G, 3G, 4G LTE, LTE-M, NB-IoT, 5G)?
- ☐ Are multi-network or steering-free roaming SIMs offered?
- ☐ Is fallback coverage available if a primary network fails?
- ☐ Does the provider have direct agreements with MNOs or rely on intermediaries?

2 SIM Type & Form Factor

- ☐ Are multiple SIM form factors offered (2FF/3FF/4FF, MFF2 eSIM, iSIM)?
- ☐ Are industrial-grade or rugged SIMs available for harsh environments?
- ☐ Is Remote SIM Provisioning (RSP) / eUICC supported?

3 Data Plans & Tariffs

- ☐ Are flexible pricing models available (pooled, pay-per-use, flat-rate)?
- ☐ Are there overage charges or throttling policies?
- ☐ Are data plans optimized for low-, mid-, or high-bandwidth IoT use cases?
- ☐ Can plans be customized per region or device type?

4 Security & Compliance

- ☐ Is data encrypted in transit and at rest?
- ☐ Are private APNs or VPNs available?
- ☐ Is IMEI/SIM lock supported?
- ☐ Does the provider comply with standards like GDPR, ISO 27001, HIPAA (if applicable)?
- ☐ Are fraud detection and usage anomaly alerts provided?

5 Management Platform

- [ ] Is a self-service connectivity management platform available?
- [ ] Can you activate, suspend, or terminate SIMs in real-time?
- [ ] Does it offer analytics, diagnostics, and usage reporting?
- [ ] Is API access available for integration with enterprise systems?
- [ ] Are automation features (e.g., rule-based alerts, provisioning workflows) available?

6 Device & Network Compatibility

- [ ] Does the provider validate modem/module compatibility?
- [ ] Are whitelists or blacklists enforced by local carriers?
- [ ] Is IMSI switching or multi-IMSI supported?
- [ ] Is the provider certified with your modem/module vendors?

7 Technical Support & SLAs

- [ ] Is 24/7 technical support available?
- [ ] Are support channels clearly defined (ticketing, phone, email)?
- [ ] Are SLAs (uptime, latency, issue resolution) clearly stated and measurable?
- [ ] Is onboarding/training assistance provided?

8 Deployment & Scalability

- [ ] Can the provider support large-scale deployments (100k+ devices)?
- [ ] Are zero-touch provisioning and remote troubleshooting supported?
- [ ] Is the platform built for global lifecycle management?
- [ ] Does the provider offer staging or pilot programs?

9 Commercial Terms

- [ ] Are minimum contract terms and commitments clearly stated?
- [ ] Are there setup fees, SIM costs, or hidden charges?
- [ ] Are volume discounts or tiered pricing available?
- [ ] What is the SIM expiration policy (inactive/dormant SIMs)?
- [ ] Can unused data be rolled over or shared across SIMs?

10 Futureproofing

- [ ] Is there a migration path from legacy tech (2G/3G sunset)?
- [ ] Are OTA firmware updates and remote configuration supported?
- [ ] Is the provider financially stable and a long-term partner?

Conclusion

Cellular IoT connectivity is more than just a technical detail, it's the backbone of any successful IoT deployment. Whether you're overseeing critical infrastructure, tracking assets worldwide, managing industrial operations, or powering smart city solutions, the strength of your connectivity directly impacts the reliability, security, scalability, and efficiency of your entire IoT ecosystem.

Selecting IoT connectivity isn't as simple as picking a SIM card or data plan. It's a strategic decision that involves evaluating multiple interconnected factors, including network coverage and resilience, SIM and eSIM flexibility, platform integration, security infrastructure, cost of ownership, and the consistency of service and support. Making informed choices in these areas ensures your devices stay connected, your data is protected, and your operations can grow with confidence.

Just as important is choosing a partner who treats connectivity as a managed service, not a commodity. The right provider offers transparency, automation, long-term adaptability, and responsive support. With the right partner, connectivity becomes a powerful tool, helping you simplify complexity, gain better control, and maximize visibility across your entire deployment.

About Pelion

Pelion

Pelion offers a comprehensive cellular IoT connectivity solution designed to meet rigorous IoT connectivity requirements. Our global multi-network SIMs include eUICC-enabled eSIM profiles for seamless carrier switching, ensuring robust coverage and resilience.

Pelion's connectivity management platform, the Pelion Portal, features an intuitive self-service portal, extensive APIs, and integrations with leading cloud providers. The solution prioritizes security through end-to-end encryption, and compliance support."

With scalable pricing, unified billing, and strong SLAs delivering industry-leading uptime of 99.995%, it doesn't matter whether you're deploying 10 devices or 100,000 across continents – Pelion enables secure, resilient, and scalable cellular IoT connectivity.

Cellular IoT Connectivity
IoT Connectivity Evaluation Framework

Helping you measure, compare, and plan your cellular IoT connectivity for short- and long-term success.

1 Understand Business Needs & Use Cases

- ☐ Define core objectives (tracking, monitoring, automation, etc.)
- ☐ Identify device types, expected volumes, and geographies
- ☐ Map requirements to business outcomes

2 Short-Term vs. Long-Term Deployment

- ☐ **Short-term:** speed of rollout, ease of integration
- ☐ **Long-term:** scalability, global coverage, contract flexibility

Pelion

3 Connectivity Technology Landscape

- [ ] Assess available technologies (2G/3G sunset, LTE-M, NB-IoT, 4G, 5G)
- [ ] Match technology to device lifecycle and data requirements

4 Connectivity Provider Selection Criteria

- [ ] Network coverage and quality
- [ ] SIM/eSIM capabilities
- [ ] Management platform and APIs

5 Vendor Stability & References

- [ ] Choose partners positioned for long-term viability
- [ ] Verify customer references and case studies
- [ ] Review financial health and market presence

6 Build a Procurement Strategy

- [ ] Align internal stakeholders (IT, procurement, operations)
- [ ] Define selection timelines and evaluation criteria
- [ ] Balance technical needs with commercial priorities

7 Evaluate Vendors: Test, Pilot, Compare

- [ ] Run proof-of-concept deployments
- [ ] Assess ease of integration and support responsiveness
- [ ] Compare performance across regions

8 Use a Scoring Matrix

- [ ] Create weighted criteria (coverage, cost, platform features, SLAs)
- [ ] Use scores to drive objective decision-making

9 Cost Models & Flexibility

- [ ] Review pricing options (per SIM, per MB, bundled plans)
- [ ] Look for flexibility as volumes and geographies change
- [ ] Check for hidden fees (roaming, activation, termination)

10 Security, Compliance & Risk Management

- [ ] Ensure compliance with local regulations (GDPR, HIPAA, etc.)
- [ ] Review encryption, authentication, and data isolation practices
- [ ] Assess vendor's incident response processes

11 Managing Scale

- [ ] SIM lifecycle management (activation, suspension, replacement)
- [ ] Roaming agreements for cross-border deployments
- [ ] Global reach through multi-network or aggregator models

12 Procurement Process Flow

- [ ] Draft RFP with clear requirements
- [ ] Shortlist and evaluate vendors against scoring matrix
- [ ] Negotiate contract terms and SLAs
- [ ] Finalize vendor and initiate rollout