SURVEY REPORT

eSIM Survey Report 2026

Published by

MOBILE WORLD LIVE

In partnership with

GLOBAL

amdocs | make it amazing

Kigen

Introduction

The eSIM is now ten years old. So how should we view this transformational technology as it enters its second decade? Has it really been that disruptive?

Well, it depends. In some spaces, eSIM is triggering profound change. Travel/roaming is the most obvious example. GSMA Intelligence stated earlier this year 60 per cent of eSIM users had used an eSIM service while travelling abroad in the previous 12 months. There is some evidence of disruption in the business space too.

But the devastating upheaval which some predicted has not happened. There has been no marked increase in consumer churn. Meanwhile, eSIM has already made an impression in IoT and aims to soon transform it.

Despite this, stakeholders believe the era of eSIM is now imminent. The GSMA believes the market is moving from acceleration to scale and reasons growing familiarity with the form-factor is set to unleash a wave of product innovation in consumer markets. In IoT, it sees the new SGP.32 standard freeing up enterprises to manage devices across countries through a single integration point.

eSIM poses fundamental questions for the mobile community. To gauge the mood, *Mobile World Live* teamed with 1GLOBAL, Amdocs and Kigen to commission this survey.

We quizzed mobile industry insiders for their views on the general state of eSIM progress, consumer attitudes, IoT, security and compliance.

Here are the results.

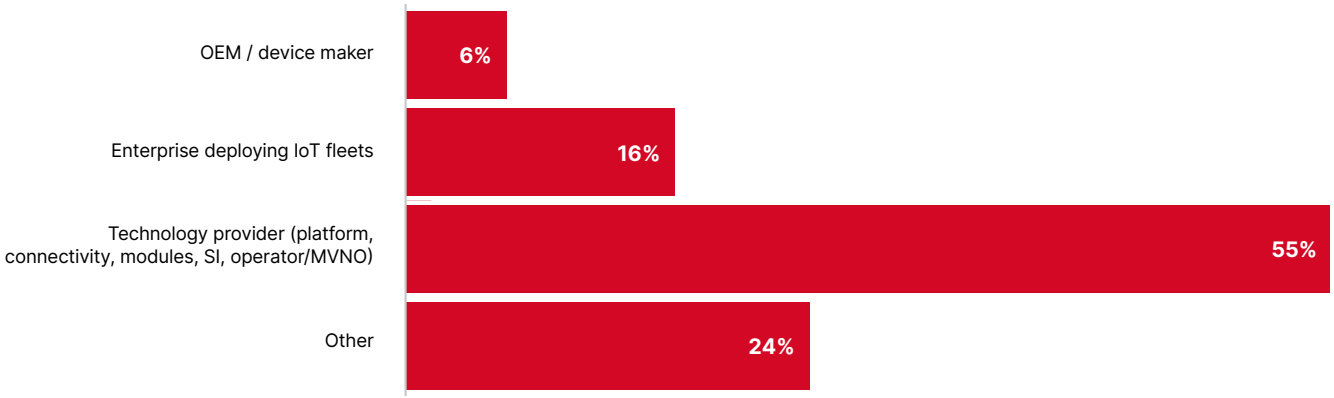
Contents

Survey participants: overview

Mobile World Live's readership spans all corners of the telecoms space. This puts us in a good position to get a holistic view of industry attitudes to specific issues. So, who took part in this study? To find out, we asked respondents framing questions about their role in the eSIM ecosystem. Here are their answers.

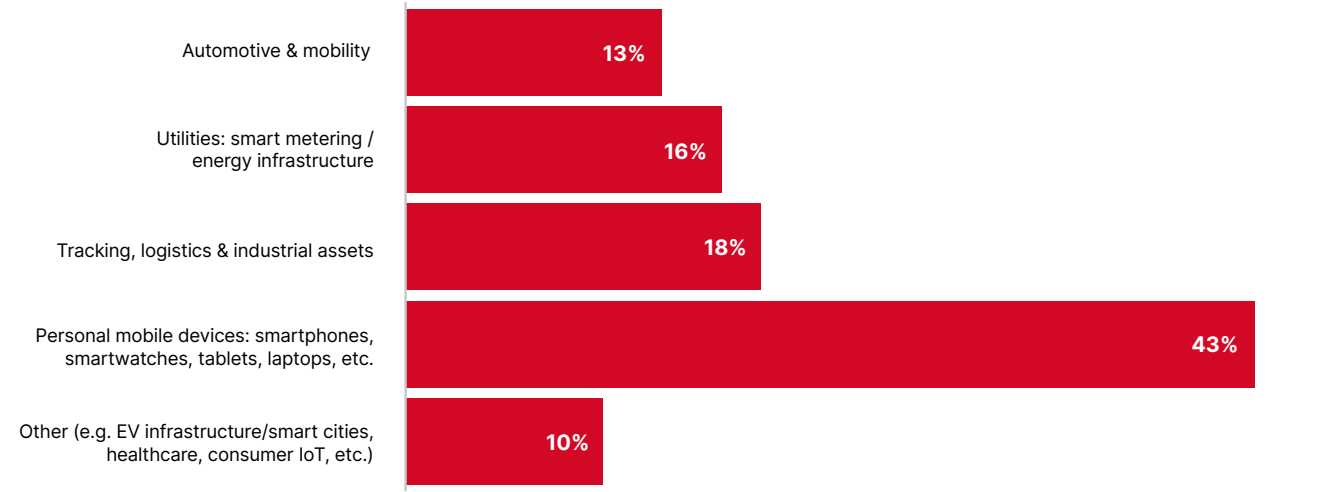
Which best describes your organisation's role in IoT eSIM adoption?

The largest group by some distance are technology providers, accounting for 55 per cent of the sample. This broad category includes MNOs and MVNOs, platform/connectivity and systems integrators. Enterprises deploying IoT fleets comprise a further 16 per cent and device makers 6 per cent. One in four identify as other.



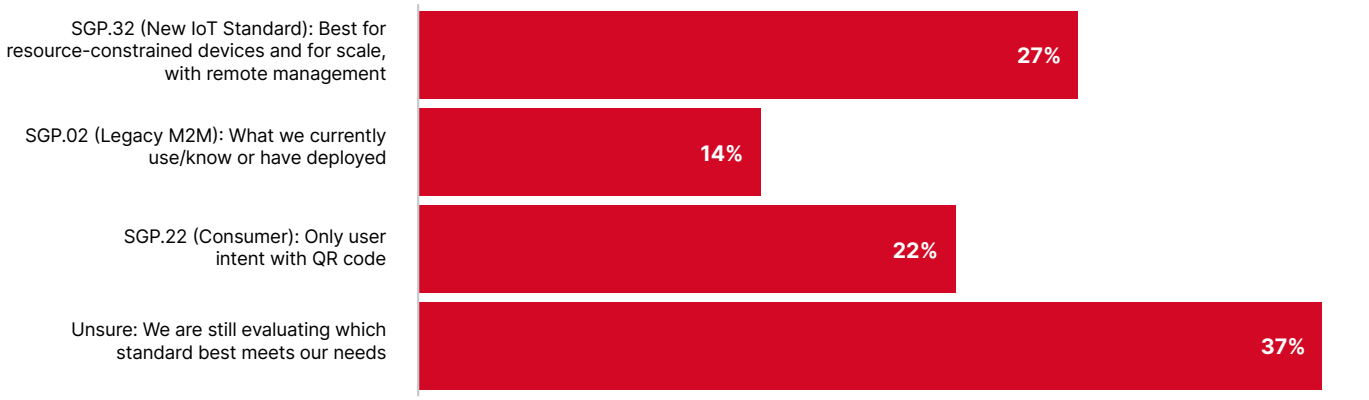
Which solution area is most likely to drive eSIM adoption for your business in 2026?

Consumer or IoT? Which is it to be? The results suggest a fairly even split when respondents were asked to select the driver of eSIM business. Personal mobile devices including smartphones, smartwatches, tablets and laptops were identified as the leading driver by 43 per cent, more than double any other category. It implies scaling eSIM in high-volume consumer channels likely presents the fastest route to revenue. But combined, the remaining industrial options accounted for 57 per cent. Tracking, logistics and industrial assets were selected by 18 per cent, with smart metering and energy infrastructure at 16 per cent, automotive and mobility on 13 per cent and other (smart cities, healthcare, consumer IoT) 10 per cent. Evidently, no single IoT segment yet dominates. Instead, IoT-driven eSIM growth appears fragmented across multiple sectors. And it is telling some markets, notably automotive, look to be stuck at the embryonic stage despite high expectations.



Which eSIM standard best fits your technical roadmap?

The new SGP.32 eSIM standard has been described as the specification which brings “consumer-like user experience to IoT operations without pretending your device has a screen, a user, or reliable power”. It is expected to have a big impact on the eSIM space. So, what do mobile stakeholders think? Which eSIM standard is in the roadmap? The responses to this question highlight a market in transition. The largest share, 37 per cent, say they are still unsure which eSIM standard is the best fit. But among the rest, SGP.32 is the leading choice, selected by 27 per cent. The result indicates that many organisations are aligning their roadmaps with next-generation IoT requirements rather than legacy approaches. The SGP.22 consumer standard was identified by 22 per cent of respondents. Only 14 per cent of respondents say legacy SGP.02 best fits their roadmap. Many organisations appear to be planning migration away from legacy M2M models toward more flexible standards.



State of the industry

IN PARTNERSHIP WITH
OUR HEADLINE SPONSOR

1GLOBAL

The smartphone is a tool for dematerialising. It took the camera, the alarm clock, the map and many more physical things and turned them into software. The result? Amazing new consumer experiences and irreversible market disruption.

Then the eSIM came along to dematerialise the SIM itself. Suddenly, the possible target of the disruption was the mobile industry itself. The eSIM is neither insertable nor swappable. It is soldered inside the device, storing an Embedded Universal Integrated Circuit Card (eUICC) which can house multiple SIM profiles containing subscriber data.

The launch of eSIM posed existential questions. Would easier switching undermine mobile network operators (MNOs) or would it help them open new markets? How would it impact roaming? What about IoT? Would eSIM make OEMs more powerful?

We're still waiting to find out. Why? Because, according to GSMA Intelligence research issued in 2026, eSIM adoption is still modest (outside of the US). But consumer interest is growing. It found 54 per cent of consumers who do not currently use eSIM are interested in using it in their smartphone at some point in the future. As a result, it expects eSIM smartphone connections to reach 4.9 billion by 2030.

For now, eSIM is making the biggest difference in the travel sector, where consumers are attracted by the low cost and on-boarding convenience of eSIM. This change in behaviour is powering big changes in supply, allowing diverse companies to enter the connectivity space. Take Revolut, for example. The digital bank teamed with eSIM specialist 1GLOBAL and now lets users access data in more than 200 regions using its app.

We seem to be at a transitional point for eSIM. Consumer interest is clearly growing. Meanwhile, in the industrial space, the SGP.32 standard is removing some of the technical barriers to adoption.

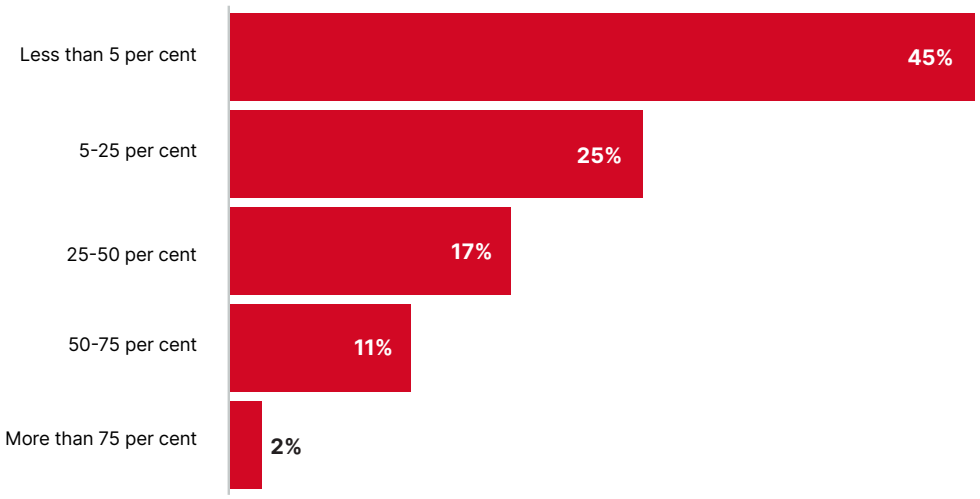
Are there reasons for optimism? Our study suggests so. It found 22 per cent of respondents are in full eSIM deployment, while 30 per cent are planning to deploy. These organisations have decisions to make around technology, partnerships, business models, roll out, which sectors to target and more. This state of the industry section reflects their current outlook.

How would you describe your organisation's current eSIM deployment?

The overwhelming conclusion of this survey finding is there is no overwhelming conclusion. Results are more or less evenly split across all options. The largest group of respondents, 30 per cent, describe their organisation as planning to deploy eSIM. This indicates that, for many organisations, eSIM has moved beyond trials but is not yet fully scaled across all relevant products or markets. That said, more than half of organisations are already live to some degree: along with those in the planning phase, 22 per cent are in full deployment and actively promoting eSIM to customers, while the same number are in limited deployment. At the other end of the scale, 26 per cent have no plans for deployment.

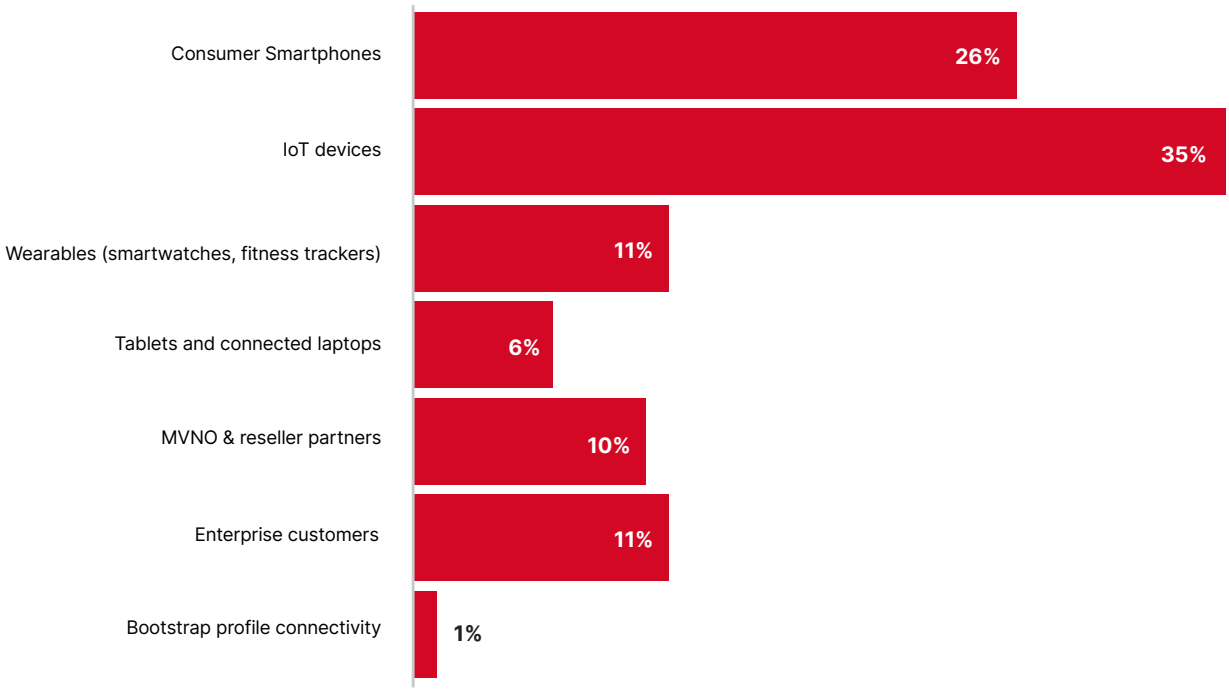
What percentage of your customer base is using eSIM-enabled devices?

GSMA research suggests eSIM had achieved 5 per cent penetration as of the end of 2025. This survey question broadly corroborates this. The largest group of respondents, 45 per cent, say fewer than 5 per cent of their customers are currently using eSIM-enabled devices. One in four rate adoption higher at between 5 per cent and 25 per cent of their customer bases. It is possible this might reflect the preponderance of iPhone owners among their subscribers. Mid-range adoption is less common: 17 per cent report penetration levels of 25 per cent to 50 per cent, while 11 per cent say that 50 per cent to 75 per cent of their customers use eSIM-enabled devices. Just 2 per cent report penetration above 75 per cent.



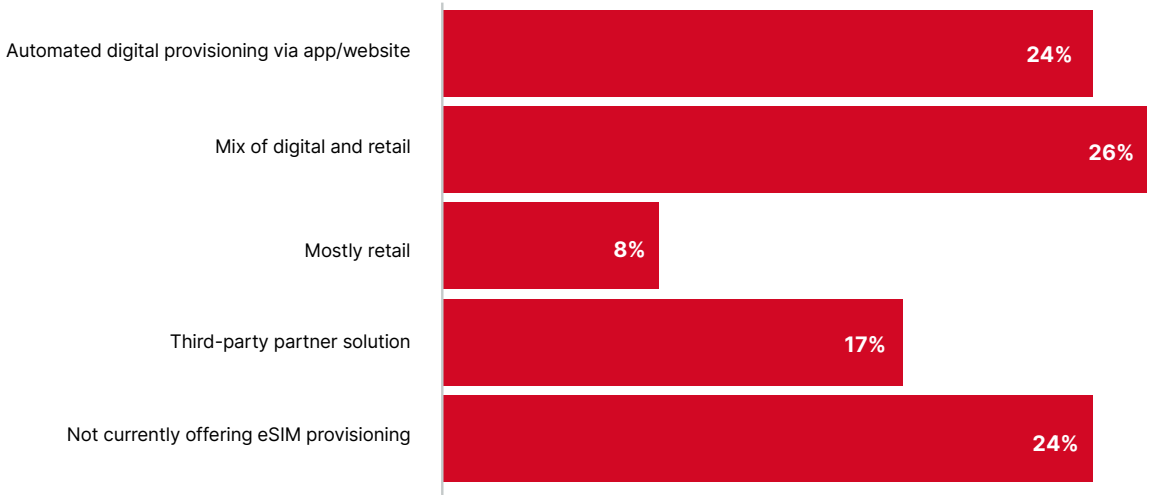
Which market segment do you believe will benefit most from eSIM adoption?

The results indicate that just under half are looking to consumer-focused markets. Smartphones are the choice of 26 per cent, with wearables at 11 percent and tablets at 6 per cent. The latter two answers possibly reflect interest in the ability of eSIM to support standalone connectivity without reliance on a paired smartphone. Away from the consumer space, 35 per cent identify IoT devices as the segment most likely to gain value. It's a fairly high number, which reflects the growing interest in eSIM for IoT. Finally, there's a modest but noticeable showing for the benefit of eSIM to MVNO and reseller partners (selected by 10 per cent of respondents). We might assume this relates to gains made by these market players in the travel eSIM space. Enterprise customers scored 11 per cent, possibly reflecting the positive contribution eSIM can make to flexible employee phone contracts.



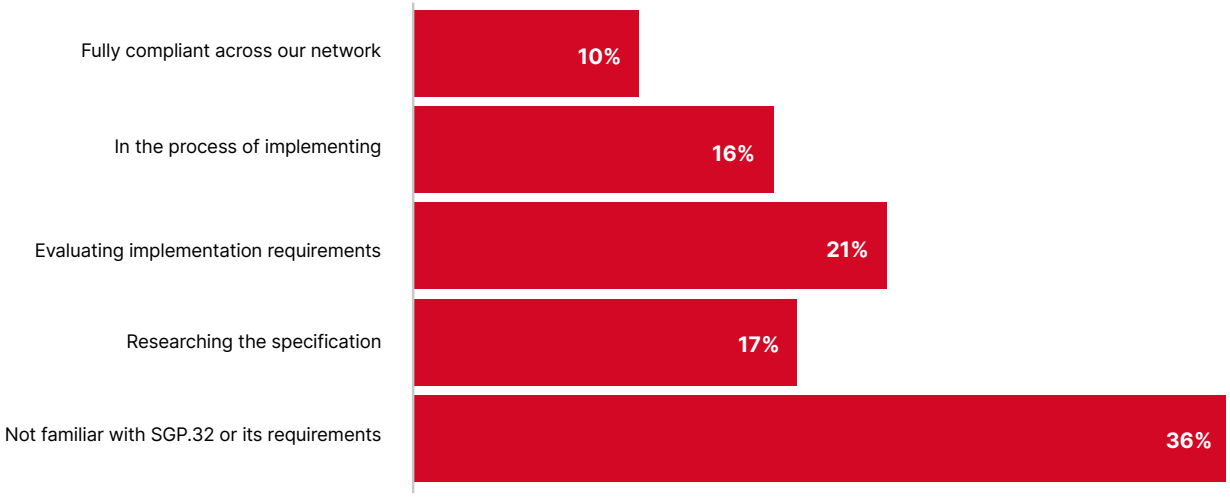
How do you handle eSIM provisioning?

The question of how to do eSIM provisioning is an important one. Why? Because even after ten years of availability, the form factor is still unfamiliar for hundreds of millions of users. Providers are certainly faced with a diversity of on-boarding choices, from all-digital to purely analogue. Our survey reveals the most common approach is a hybrid model: 26 per cent of respondents use a mix of digital and retail channels. This probably makes sense, as it supports the benefits of digital provisioning while also catering for customer groups which are less digitally confident. Fully automated digital provisioning through apps or websites is used by 24 per cent, with mostly retail at 8 per cent. Of course, another option is to outsource the task of provisioning altogether. Our survey found 17 per cent to be using third-party partner systems to bring new eSIM users onboard. Finally, it should be noted just under one in four are not currently offering eSIM provisioning at all. It seems a significant portion of the market is still at a very early stage of operational eSIM readiness.



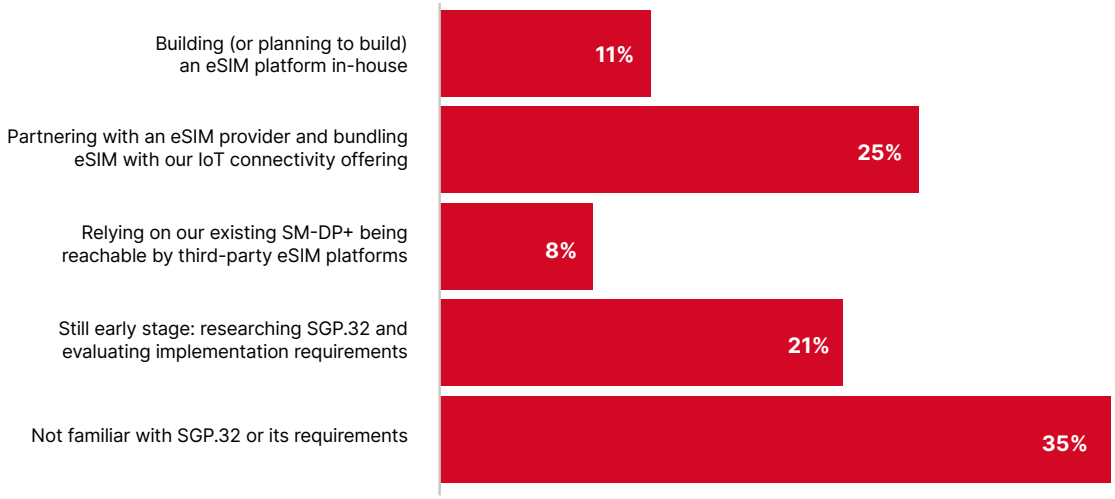
How ready are you for the SGP.32 specification?

SGP.32 is the next-generation standard for large-scale IoT eSIM deployments. It was introduced in 2023 and tested throughout 2024 and 2025. In 2026, it should go from pilot phase to mass commercial deployment. Is the industry ready? The survey suggests awareness is limited. The largest group of respondents, 36 per cent, say they are not familiar with SGP.32 or its requirements. A further 21 per cent are researching the specification, while 17 per cent are evaluating how to implement it. More advanced readiness is less common: 16 per cent are in the process of implementing and only 10 per cent report being fully compliant across their network.



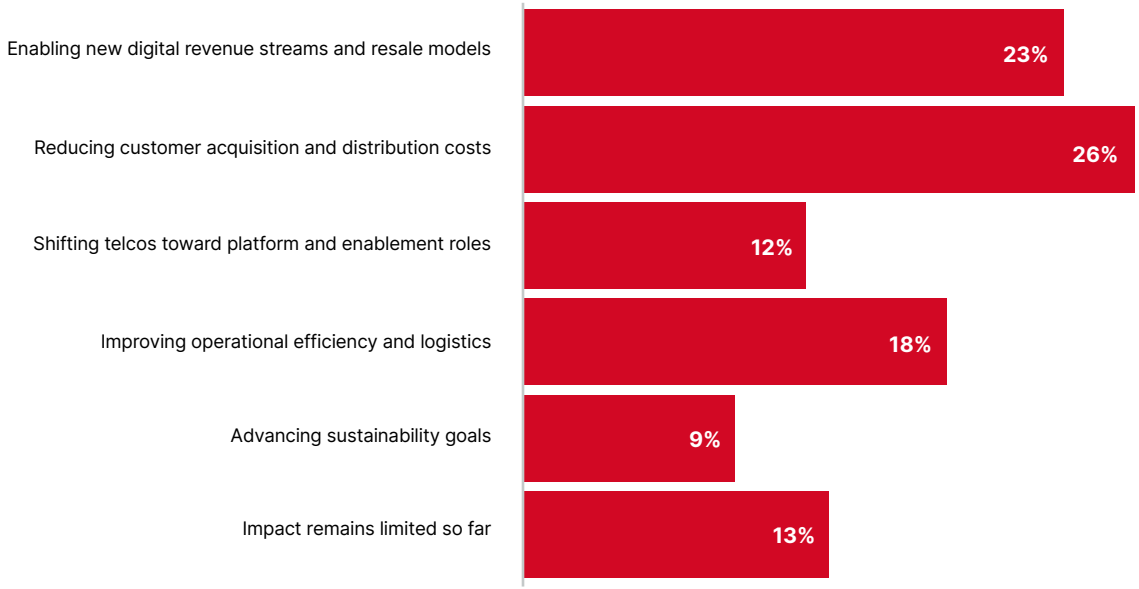
With the introduction of SGP.32 and the expansion of eSIM into IoT, which best describes your organisation's current approach?

Most organisations are still in a pre-scale phase when it comes to SGP.32. Given this, what are their plans for how to roll out live services? The majority have no concrete plans: 35 per cent are not familiar with the requirements and 21 per cent are still researching the space. So, what of the rest? The biggest group, 25 per cent, plan to partner with an eSIM provider and bundle it into their existing IoT connectivity offering; 11 per cent intend to build their own eSIM platform; and 8 per cent are confident they can rely on existing SM-DP+ being reachable by third-party eSIM platforms.



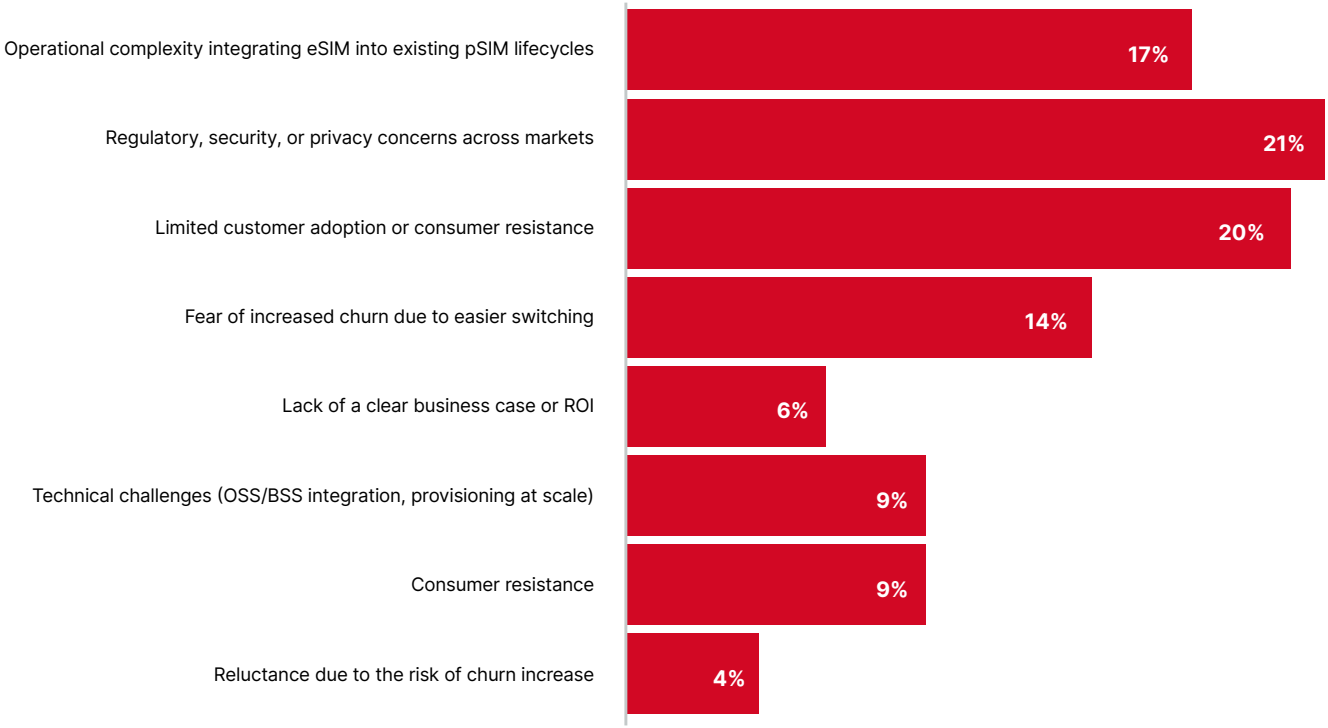
How is eSIM most positively impacting the telco business model today?

After ten years, the industry has enough experience of eSIM to judge where it has made the most positive impact. Our study reveals cost to be the number one factor, but not by much. The largest share of respondents, 26 per cent, say eSIM is reducing customer acquisition and distribution costs (eliminating physical SIM logistics, retail handling, shipping, et cetera). Meanwhile, 18 per cent point to better operational efficiency and logistics. Combined, that is 44 per cent of respondents highlighting savings of some kind. Just 9 per cent name advancing sustainability goals (reduced plastic and shipping) and 13 per cent say the impact of eSIM has been too limited to draw a clear conclusion.



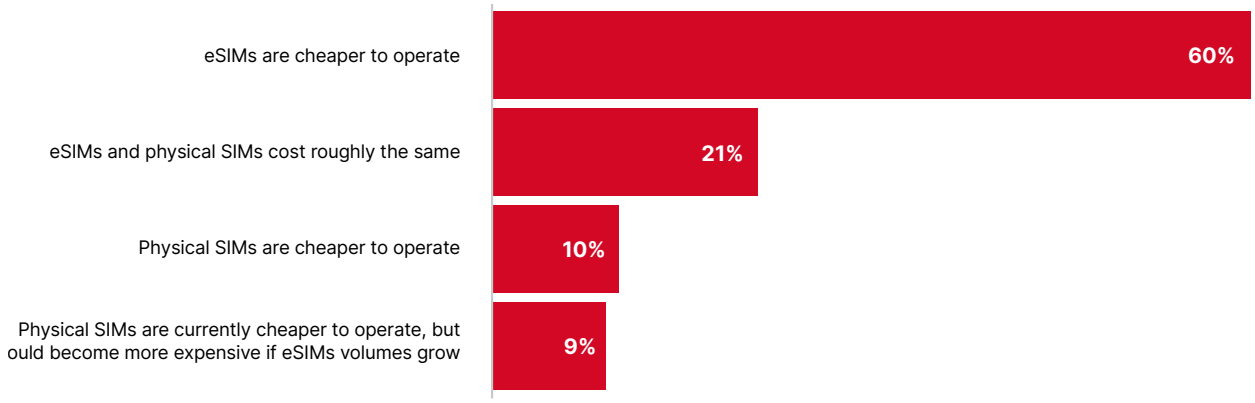
What is the biggest challenge telcos face when scaling eSIM globally?

The survey suggests that the challenges of scaling eSIM are equally balanced between operations and compliance, and consumer behaviour. The most frequently cited issues are regulatory, security and privacy concerns (21 per cent), while 17 per cent are challenged by integrating the eSIM into existing physical SIM lifecycles. On the consumer side, limited adoption/resistance is identified by a combined 29 per cent of respondents, while 14 per cent are worried about churn. Secondary challenges include a lack of a clear business case or RoI (9 per cent) and technical challenges such as OSS/BSS integration and provisioning at scale (9 per cent).



How are eSIM operational costs when compared to physical SIM?

The received wisdom is eSIM cuts costs. What do our respondents think? The results are emphatic: 60 per cent agree eSIMs are cheaper to operate than physical SIMs today. That is three-times more than those who think eSIMs and physical SIMs cost roughly the same (21 per cent). Only 10 per cent believe that physical SIMs are currently cheaper to operate, while an additional 9 per cent think this disparity will disappear as eSIM volumes grow. The results suggest that, for most stakeholders, eSIMs' advantages in terms of logistics, distribution and raw materials are already paying off.



1GLOBAL

Sponsor comment:

As headline sponsor, 1GLOBAL sees these results as clear evidence the industry is moving beyond eSIM ambition toward practical execution. While many organisations are still in early deployment, the direction is clear: eSIM is becoming a strategic enabler of more flexible, software-defined connectivity models across consumer, enterprise and IoT markets.

The opportunity goes far beyond digitising the SIM. eSIM enables simplified global service delivery, reduced operational complexity, faster time to market, and new commercial models across channels and geographies.

Findings on deployment intent, provisioning models, cost efficiency and SGP.32 readiness point to one key conclusion: scale will depend on strong infrastructure, seamless interoperability and precise execution.

At 1GLOBAL, we take an eSIM-first approach to enable new business models across the connectivity ecosystem. As a full MVNO with a global core network, we support enterprises, digital platforms and connectivity providers with solutions spanning workforce and IoT connectivity, eSIM provisioning, entitlement infrastructure and embedded telco APIs across 190+ countries.

As eSIM adoption accelerates, the winners will be those who treat connectivity not as a standalone product, but as an integrated, programmable layer of their business with eSIM at its core.

"The GSMA survey's findings on deployment intent, provisioning models, cost efficiency and SGP.32 readiness all point to one conclusion: scale will depend on strong infrastructure, seamless interoperability and precise execution."

Raghav Rajpal, Growth Marketing Lead, 1GLOBAL

1GLOBAL

1GLOBAL is a full MVNO that leverages a unified connectivity solution, enabling businesses to operate seamlessly across 190+ countries with our single core network infrastructure, enhancing global reach and operational flexibility.

Explore our solutions

- Employee Connectivity
- SIM Provisioning (SM-DP+)
- POS & Retail Connectivity
- Compliance & Recording
- Entitlement Server
- IoT Connectivity
- Embedded Telco & API
- SGP.32 eSIM IoT Manager

Consumer eSIM: Customer Behaviour

IN PARTNERSHIP WITH

amdocs | make it amazing

Shortly after eSIM was launched in 2016, one industry analyst published a report entitled eSIM: Harbinger of doom or bringer of hope? It was a suitably dramatic headline, reflecting the dread/excitement surrounding the new form-factor in consumer-facing spaces. The article explained the transition to eSIM is already underway and operators must adapt by investing in digital capabilities, partnerships and new value propositions. Should they fail to do so, they risk irrelevance.

So which prediction was correct?

On balance, you would have to say hope won. There has been little evidence of doom. eSIM was deployed first in the Samsung Gear S2 Classic 3G smartwatch, but moved past an inflection point after the release of the US-exclusive, eSIM only iPhone in 2022. However, the expected rise in consumer churn inspired by the ability to click a menu item to change carriers never materialised. Indeed, in 2025, GSMA Intelligence reported eSIM has no impact on churn even in the US where there has been rapid adoption.

So limited doom. But what about hope. Well, as explained in the previous chapter, eSIM has ignited the travel market. While specialist OTT third parties are playing a part in this, a growing number of MNOs are embracing the opportunity too. For example, Vodafone Group has launched its own travel eSIM product in more than 200 countries.

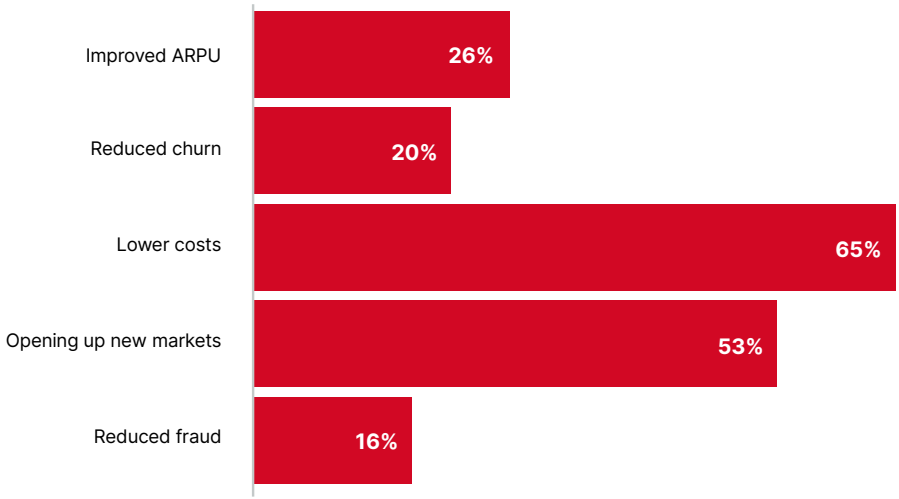
There has also been a gradual proliferation of consumer eSIM devices. The form-factor certainly expands the opportunity for MNOs to sell connectivity in new spaces (fitness, wearables, watches et cetera). At the end of 2024, there were 271 eSIM devices available. Insiders expect more mid- and low-price phones to support eSIM soon. They also believe MNOs will start to prioritise eSIM when onboarding new customers. This will be made easier by the launch of cloud-native SaaS systems from specialists like Amdocs which simplify activations, subscription management, entitlements and more.

While the eSIM makes the consumer experience better in many ways, it adds complexity in others. It asks users to manage a digital profile across a range of scenarios such as device transfer, profile deletion, upgrades, migration from physical SIM to eSIM, temporary device use (such as travel) and handling lost or stolen devices. Telcos must find a way to meet this challenge.

In this chapter, we try to get a sense of the place of eSIM in consumer markets. The results explore the benefits, use cases, costs and more. And they reveal the most prominent obstacle to adoption might be a simple lack of awareness: 55 per cent of respondents believe their customers do not know eSIM exists. So, lots of work to do, but good evidence it pays off.

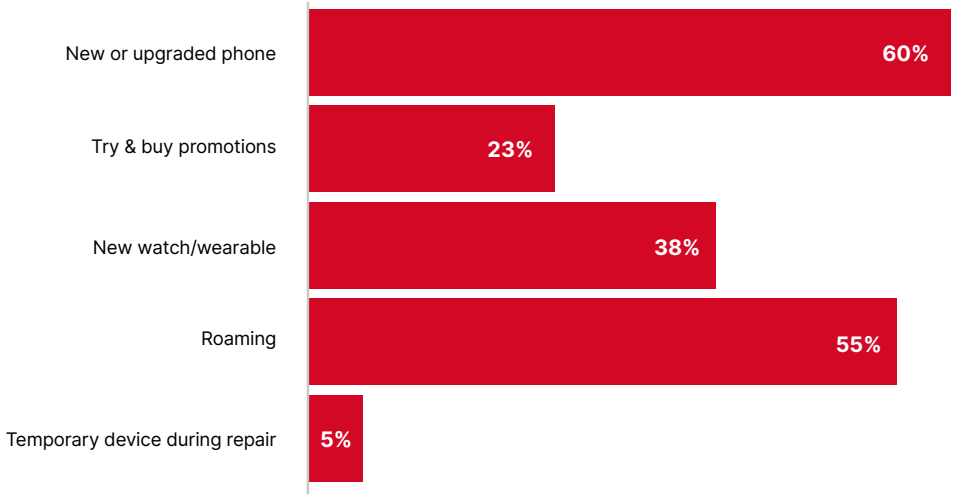
What is the main business benefit of migrating your consumers to eSIM?

Two factors stand out when it comes to the benefits of a transition to consumer eSIM: cost and access to new markets. Survey answers reveal the primary business benefits of migrating consumers are focused on operational efficiency and market reach rather than revenue increases. 65 per cent of respondents cited lower costs, while 53 per cent highlighted opening new markets. These benefits hugely outweigh ARPU, reduced churn and anti-fraud (26 per cent, 20 per cent and 16 per cent, respectively).



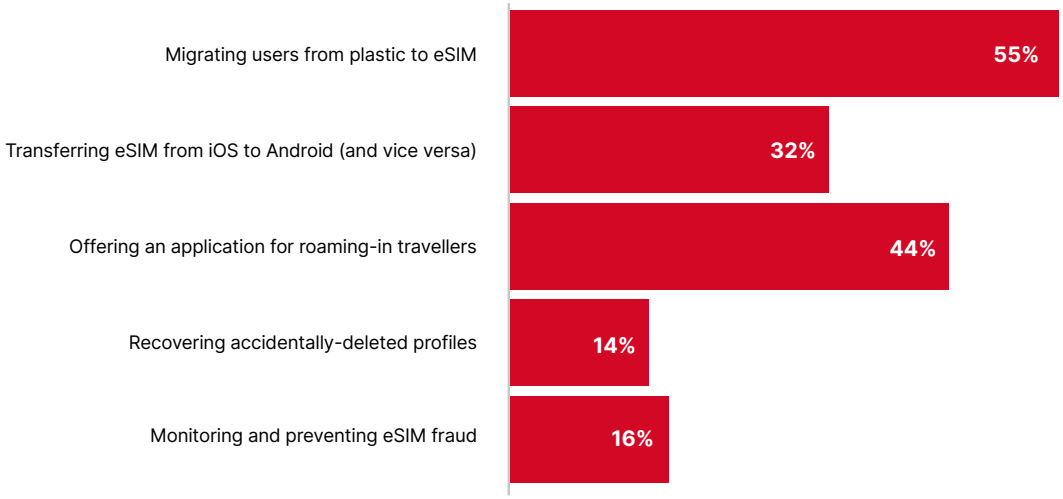
What are your primary use cases for consumer eSIM?

Why would a consumer upgrade to eSIM? The most prominent use case is setting up a new or upgraded phone, cited by 60 per cent of respondents. Unsurprisingly, roaming is a close second, identified by 55 per cent. Travel is widely acknowledged to be a boom space for eSIM thanks to widespread product innovation. Elsewhere, 38 per cent of respondents point to watches or wearables as a trigger for eSIM adoption, while 23 per cent point to try and buy promotions. Just 5 per cent see eSIM as a useful for connecting temporary devices during repairs.



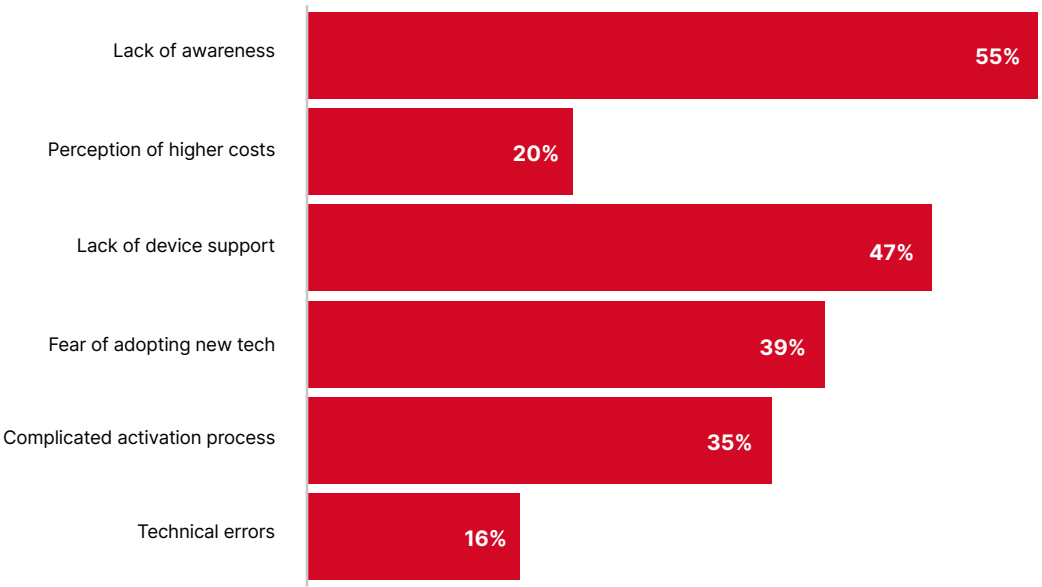
Which eSIM management features do you currently offer?

eSIM fundamentally changes on-boarding and connectivity processes. So which management functions are respondents now offering? The most prevalent feature is the ability to migrate users from plastic to eSIM (provided by 55 per cent). 44 per cent have responded to the travel opportunity by offering dedicated eSIM applications for roaming customers. Around a third support transferring eSIMs between iOS and Android platforms. Smaller numbers support preventing eSIM fraud and recovering accidentally deleted profiles (16 per cent and 14 per cent, respectively).



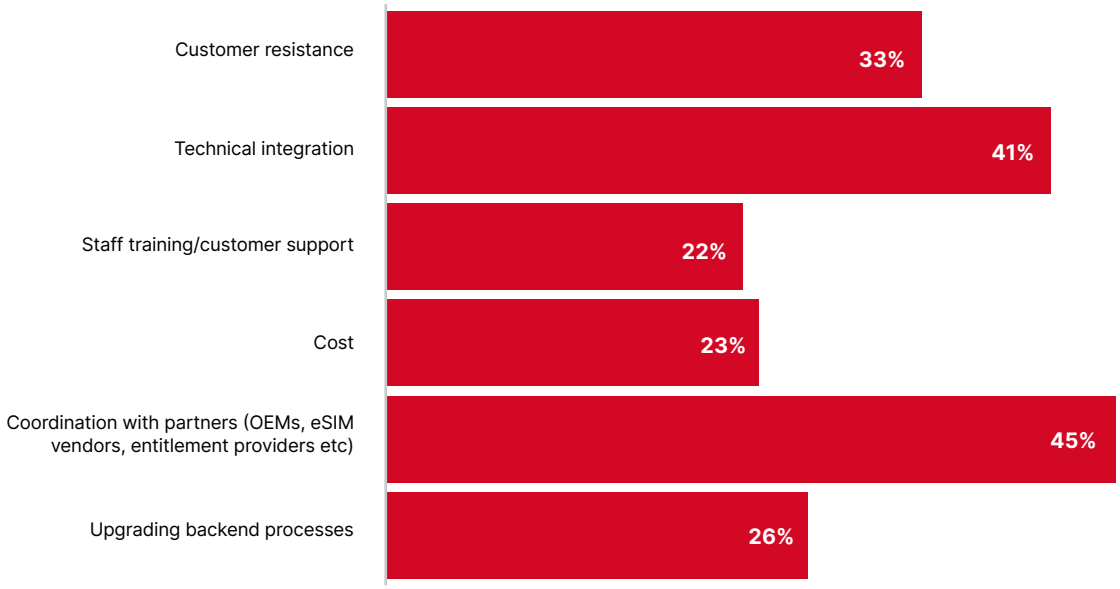
What are the key barriers to consumer adoption of eSIM?

Ten years after the arrival of eSIMs the form-factor is not exactly universal in the consumer-facing mobile space. Why not? The most prominent obstacle is a simple lack of awareness, identified by 55 per cent of respondents. This indicates further education is needed to remind consumers eSIM even exists. That said, 47 per cent cited a lack of device support as a key barrier, so maybe a dearth of awareness is understandable. The other reasons are more to do with psychology: 39 per cent say fear of adopting new technology is an issue, while 35 per cent highlighted the complicated activation process. 20 per cent believe a perception costs are higher is a barrier and 16 per cent say technical errors might be putting users off.



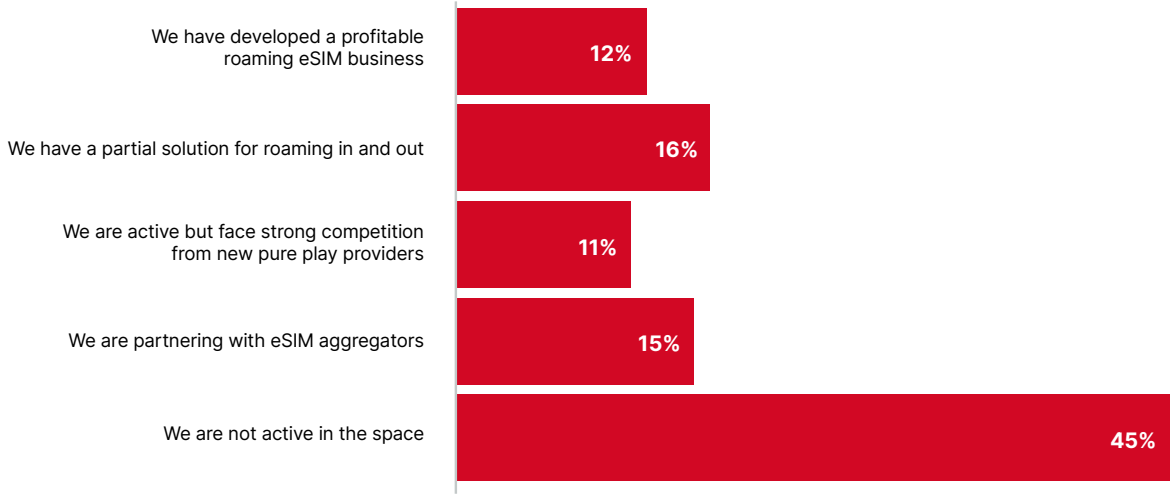
What are the main challenges in rolling out eSIM?

Assuming respondents are convinced of the benefits of supporting eSIM, what might stop them rolling it out? Short answer: complexity. 45 per cent cited the challenge of coordination with OEMs, eSIM vendors and entitlement providers. In a related finding, 41 per cent highlighted technical integration, while 26 per cent mentioned upgrading backend processes. Around 33 per cent think customer resistance is a significant obstacle and 23 per cent costs.



How would you describe your eSIM roaming activity?

The eSIM travel market might be booming, but it is far from saturated. Our study revealed nearly half (45 per cent) of respondents are not yet fully active in the eSIM roaming sector. Of those which are, 16 per cent describe their status as having a partial solution. Another 15 per cent are partnering with eSIM aggregators to manage their roaming services. 12 per cent of respondents report a profitable roaming eSIM business, while 11 per cent are live, but face pressure from pure play providers.



Sponsor comment:

The findings highlight a clear inflection point in the evolution of eSIM. But the real story is no longer about adoption, it's about execution. While many operators still approach eSIM as a physical SIM replacement, the bigger challenge lies in turning it into a scalable, revenue-generating digital platform.

What is holding operators back is not technology, but the complexity of managing the eSIM lifecycle across fragmented domains. Device changes, profile transfers, entitlement handling and recovery flows often break the customer experience. Meanwhile, behind the scenes, operators struggle to coordinate across OEM dependencies, provisioning systems and disconnected entitlement layers. This lack of real-time control creates operational friction, limits agility and ultimately constrains monetisation.

At the same time, digital-first disruptors, especially in roaming and travel eSIM, are capitalising on these gaps. They are setting new benchmarks for simplicity, speed and user experience while increasing the risk of disintermediation.

This is exactly where Amdocs eSIM Cloud makes the difference. As the industry's number one eSIM platform, Amdocs provides a cloud-native platform which unifies orchestration, entitlement and provisioning into a single, real-time layer. It enables operators to fully leverage OEM, device and service capabilities to deliver a seamless, end-to-end consumer experience. By simplifying complex lifecycle journeys and enabling real-time, API-driven control, Amdocs empowers service providers not just to reduce cost, but to unlock new growth, accelerate partner innovation and compete effectively in a digital-first ecosystem.

The #1

Entitlement Server & Orchestration Platform

Amdocs eSIM Cloud

a· | make it amazing

a·OS | Agentic Operating System for Telco

Enterprise: IoT

IN PARTNERSHIP WITH

Kigen

eSIM would seem tailor-made for the Internet of Things. The swappable plastic SIM is not a good fit for devices which might need to travel to a remote overseas location or move across multiple networks. A pre-loaded eSIM would appear to solve all these problems: just configure it in the factory with In-Factory Profile Provisioning (IFPP) or use Remote SIM Provisioning (RSP) to change network profiles over-the-air later.

That is the theory. The practice is a little different. Legacy eSIM standards including SGP.02 were designed for an earlier iteration of the IoT based on machine-to-machine (M2M) modules. SGP.02 was often locked into specific MNOs and vendors. It also struggled to connect constrained devices with limited memory or on low power, wide area networks and employed a complex interconnect process. As a result, M2M eSIM made a modest impact on the IoT, with most deployments in the automotive sector. Analyst company Kaleido estimates 280 million IoT devices actively used eSIM at the end of 2024.

Expectations are now growing thanks in part to the new SGP.32 eSIM standard. It was carefully designed to address all the shortcomings of its predecessors, enabling finer control of how an eSIM connects and operates on a network. It features more scalable interfaces, supports direct and indirect profile downloads, and lets enterprises easily select the carrier profile on the eSIM remotely.

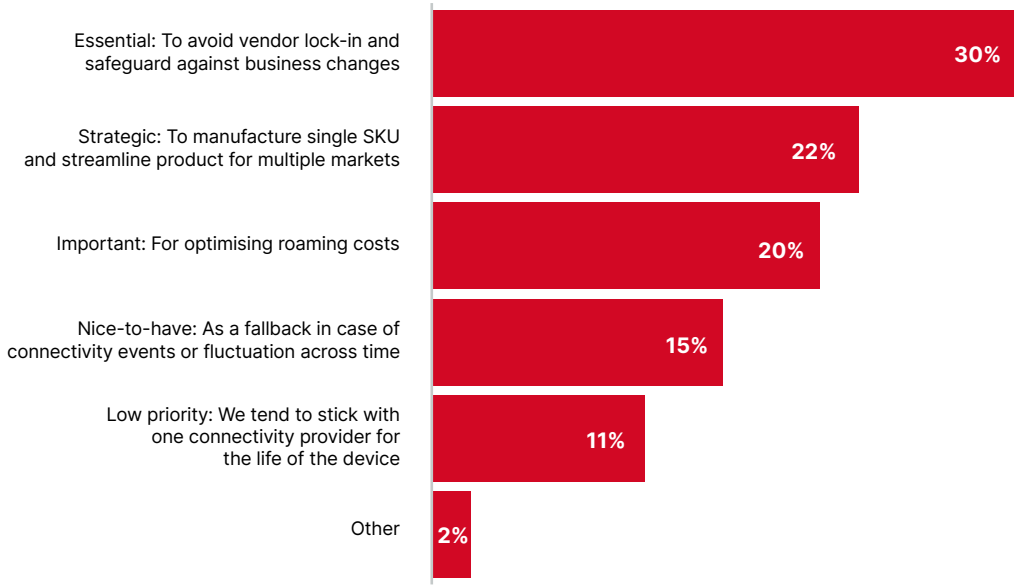
In other words, SGP.32 supports build-once, ship-anywhere. Specialist providers such as Kigen already offer an SGP.32-certified eSIM for IoT Manager (eIM) which helps enterprises quickly migrate to SGP.32 and take advantage of its innovative features fine-tuned for the global ecosystem of cellular LPWAN and 5G networks.

The incentive driving these improvements is the opportunity to extend connectivity to billions of devices across a wide range of industrial sectors. The automotive and utilities industries have already embraced smart connectivity. Indeed, the automotive IoT market size was estimated to be worth $188.4 billion in 2025. But providers are increasingly exploring the opportunity to deploy sensors and mobile asset tracking in agriculture, shipping, energy and more.

eSIM stakeholders have decisions to make. They need to factor in which eSIM form-factor to use, how and when to deploy SGP.32, when to activate profiles, who will run the eSIM IoT remote management service and more. This chapter dives into these questions.

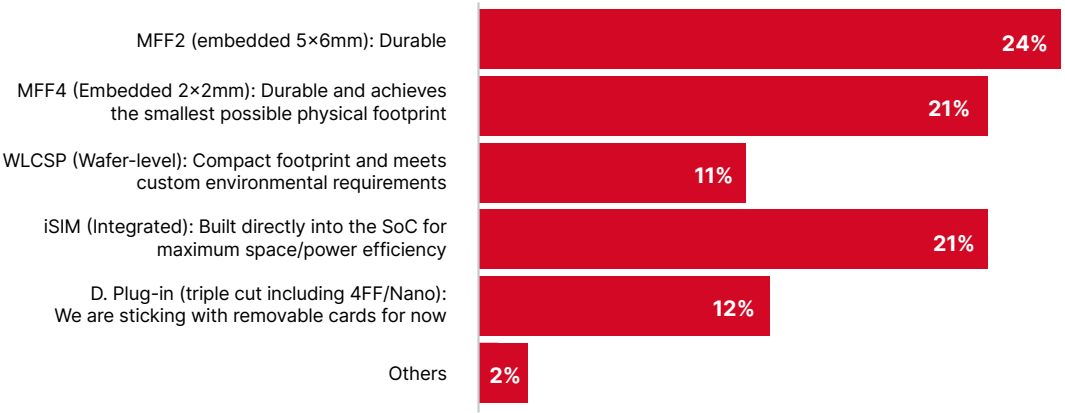
How important is it to be able to switch connectivity provider remotely over the IoT device lifecycle?

The ability to switch provider is a key component of the IoT space, where devices are often in remote or even overseas locations. So, this facility can serve multiple purposes for the enterprise. In the survey, half of respondents rate the ability to switch connectivity provider remotely as either important or essential. 30 per cent view it as essential, primarily to avoid vendor lock-in and to insure operations against future changes. 22 per cent describe it as strategic because it lets them make a single SKU. 20 per cent cite remote switching as important for optimising roaming costs, while 15 per cent consider it a nice-to-have fallback when connectivity drops. Just 11 per cent say switching is a low priority because they are sticking with a single connectivity provider.



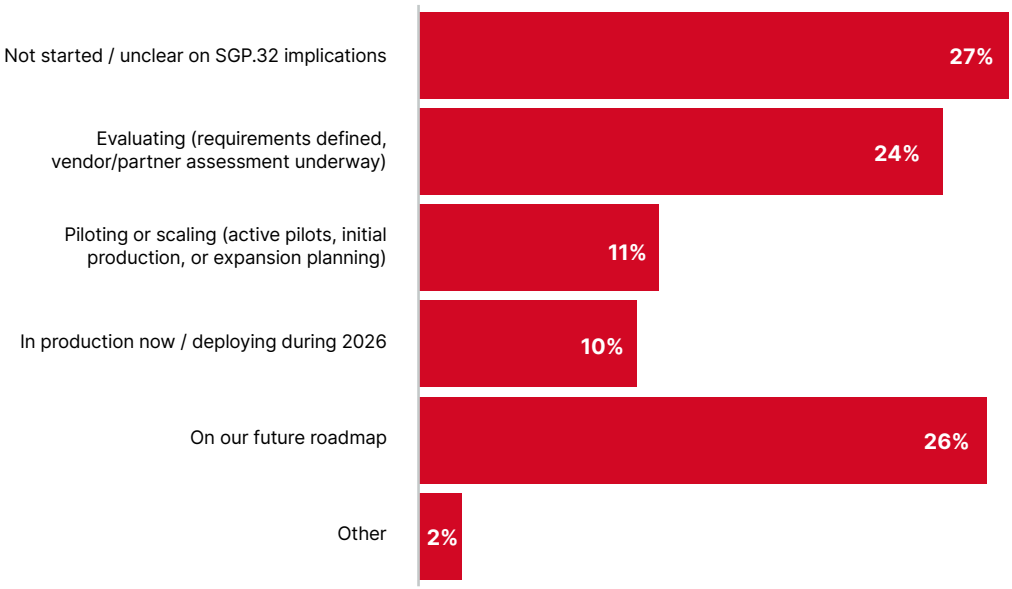
Which eSIM form-factor is your primary focus for upcoming IoT designs?

There is more than one eSIM form-factor. So, which do respondents favour in the IoT deployments? No single option is winning outright. This is understandable due to the wide range of products available in the IoT category. The most popular choice, but only just, is the MFF2 soldered or embedded form-factor. It was cited by 24 per cent and is favoured for its durability. Close behind, two technologies were backed by 21 per cent of respondents: MFF4, another soldered or embedded form factor (measuring 2mm x 2mm) and iSIM (integrated directly into the System on a Chip) are backed for their small physical footprint and efficiency. Less favoured is Wafer-level Chip Scale Package (WLCSP) at 11 per cent. Finally, 12 per cent report sticking with the traditional D. Plug-in triple-cut cards (including 4FF/Nano) for the time being.



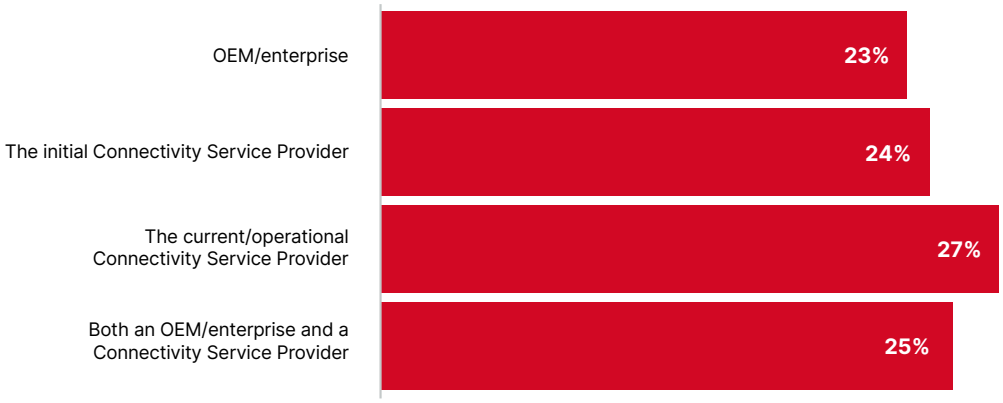
What is your current status regarding SGP.32-based remote provisioning?

SGP.32 is expected to shake up the eSIM IoT space, making it easier to remotely provision and manage constrained IoT devices through secure servers. The standard was launched in 2025 with first certifications available from mid-year, so it is embryonic for now, which the survey makes clear. Just 10 per cent report being in full production or planning to deploy during 2026. At the other end, 27 per cent have not started and are still unsure about SGP.32 and its ramifications. This leaves 61 per cent in varying stages of preparations. 24 per cent are evaluating, while 26 per cent have included SGP.32-based provisioning on their roadmaps. 11 per cent of organisations are piloting or scaling the technology.



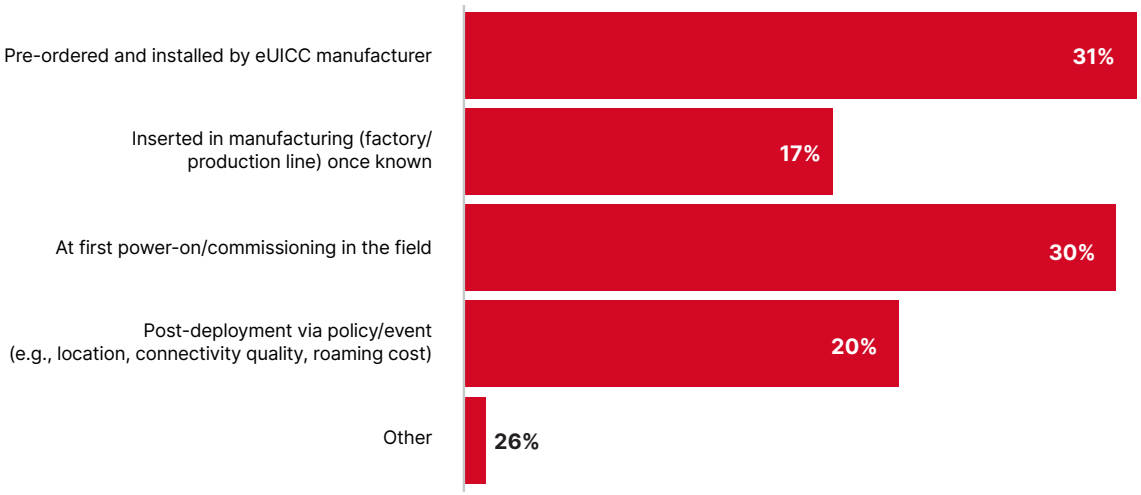
If you're considering SGP.32, who will run the eSIM IoT remote management service?

SGP.32 might simplify deployments but it does demand a new approach to eSIM logistics and management. It begs the question: who should handle remote activations and activities? The study suggests there is no consensus. Indeed, there was an almost even split across all options. The most common expectation, at 27 per cent, is the incumbent provider will manage the service. However, 25 per cent believe an OEM will share the responsibility. 24 per cent expect the initial connectivity service provider to run the remote management service, while 23 per cent anticipate the OEM or enterprise will handle it independently.



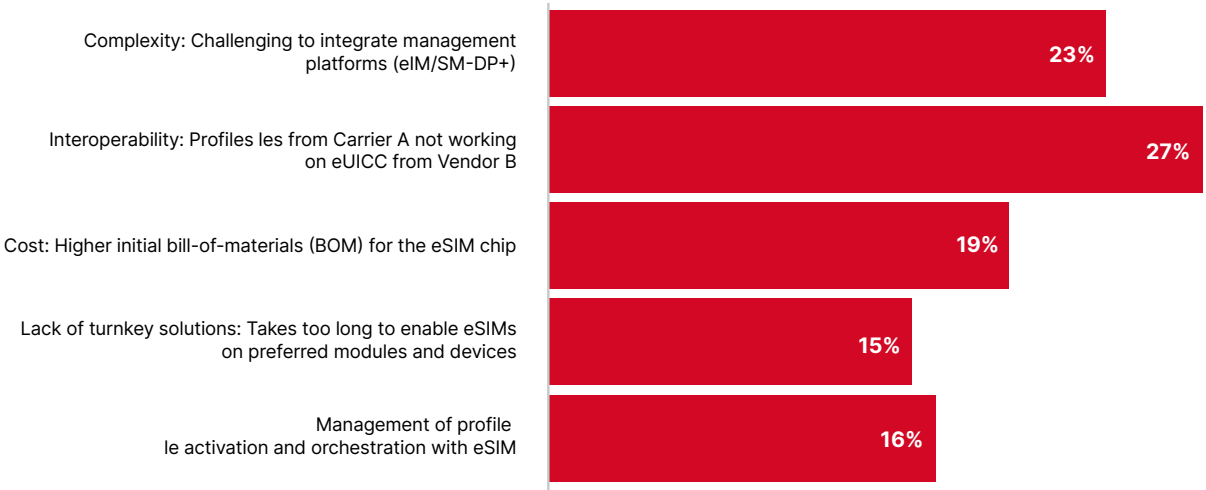
Where do you expect the primary profile download/activation to occur for most devices?

Organisations face a choice when it comes to profile activation for IoT devices. Simply put, the question is at which stage of the production or operational lifecycle should this happen? 48 per cent favour manufacturing/factory-stage provisioning. This comprises 31 per cent which believe the primary profile will be ordered and installed by the eUICC manufacturer and 17 per cent which expect the profile to be inserted during the manufacturing process on the factory or production line once the destination is known. Meanwhile 30 per cent expect to activate profiles at the first power-on in the field. And 20 per cent believe activation will occur after deployment, triggered by specific policies or events including location changes, connectivity quality or roaming costs.



What is your biggest technical hurdle to IoT eSIM adoption?

On paper, eSIM solves many of the problems facing the IoT. So, what is stopping telcos from embracing it? The answers suggest most of the sticking points are technical: 27 per cent identified interoperability as their biggest challenge, specifically when profiles from one carrier do not work on an eUICC from a different vendor. 23 per cent cited the difficulty of integrating different management platforms, for example eIM and SM-DP+, while 16 per cent point to problems with profile activation and orchestration. For 19 per cent, the main challenge is much more straightforward: cost.



Kigen

Sponsor comment:

The survey reinforces a clear market direction: IoT eSIM adoption is gaining momentum, with strong interest in SGP.32, growing recognition of the strategic value of scaled remote lifecycle management and increasing emphasis on in-factory profile provisioning. It also highlights the industry's next challenge: improving interoperability, governance, compliance and long-term cybersecurity resilience at scale.

This is closely aligned with Kigen's vision. We believe secure remote management for IoT eSIMs should be simple, scalable and built for the realities of long-life connected devices. The belief has shaped our contribution to the industry-wide collaboration behind the GSMA SGP.32 standard.

Kigen is well positioned to help organisations move from evaluation to deployment. Our latest eSIMs support SGP.22 and SGP.32, while our award-winning hosted eIM is certified for SGP.32 and is currently interoperable with more than 60 IoT modules and multiple industry SGP.32 solutions. Across M2M, consumer and automotive use cases, our portfolio is available in MFF2 and MFF4 form factors, with support for in-factory profile provisioning and remote security patching.

For connectivity providers and enterprises alike, this is an opportunity to move early, address long-term security readiness in line with emerging cybersecurity regulations and build secure services from factory provisioning onward.

GLOBAL PRODUCTS WITH IoT eSIMs

Manufacturing scale made simple.

As the industry's unrivalled forerunner in power-efficient IoT, Kigen is the trusted partner for IoT pioneers across smart energy, logistics, physical AI, and more. Secure architecture that gives predictable results for scale, with

- *GSMA certified SGP.32 eIM management solution and eSIMs*
- *Unparalleled global terrestrial and satellite connectivity ecosystem*
- *Late-stage device provisioning in the factory*
- *Security built for the future of EU Cybersecurity resilience Act and NIST-2*

Kigen invites you to discover what's possible, together.

Start today, visit kigen.com

Kigen

Let's meet

#FutureofSIM

Enterprise security and compliance

IN PARTNERSHIP WITH

Kigen

Demand for physical AI training, smart meters and automotive applications is driving growth in the IoT. But this activity raises many security challenges: permanent connectivity over the public internet opens IoT devices to new threats.

In the world of removable SIM cards, the main risk is physical tampering. Stakeholders have addressed many of these issues through industry-wide schemes (along with additional security measures) which test emerging threat scenarios. However, no testing can ever be exhaustive. With the advent of eSIM, the key question becomes how the security models which serve plastic SIMs can be upheld and strengthened to address the logistics, governance and ownership of the new form-factor.

The stakes are even higher in industrial contexts, where devices may connect to critical infrastructure. There are also deployment approaches in which the push model of remote provisioning does not always assume devices are continuously online.

It is incumbent on the industry and its customers to address these issues. The good news is eSIMs which adhere to GSMA certifications offer in-built protections against known vulnerability and security threats. The hardware Root of Trust (RoT), for example, ensures the device can securely authenticate itself to the network using private keys and cryptographic functions. Meanwhile, there are best practices to follow: implementing multi-factor authentication for remote provisioning, establishing secure boot processes, maintaining regular security patch management and so on.

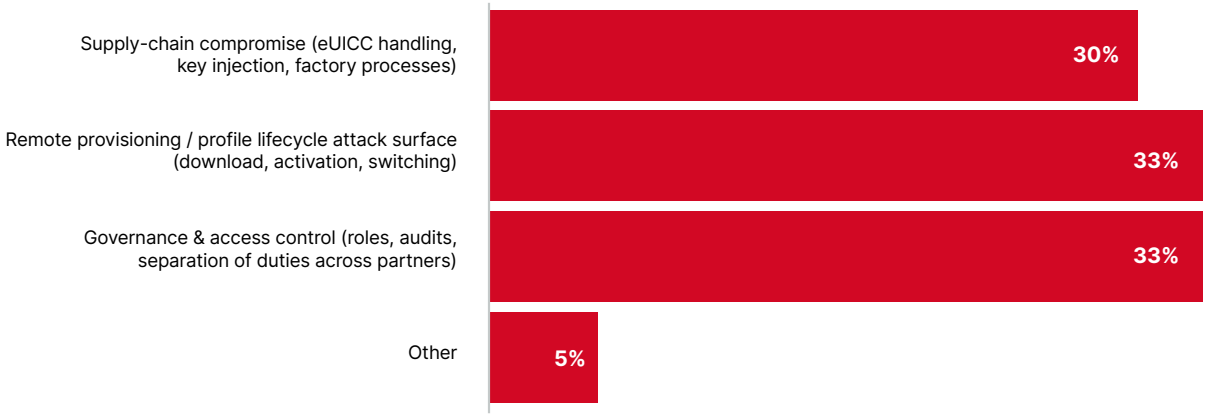
The regulatory landscape is also evolving to address cybersecurity challenges and all IoT stakeholders are directly impacted. The European Union's Cyber Resilience Act (CRA) is focusing minds across the sector. It mandates device makers update the security of devices using digital elements for up to five years and maintain documentation on vulnerabilities for longer. It will fully apply by December 2027 although reporting obligations begin from September 2026.

To get ahead of all these challenges, specialist providers such as Kigen are aligning the latest standard-certified eSIMs to offer programmes which ensure IoT product owners and manufacturers can meet the required obligations of the CRA expediently.

In this final section of the study, we explore how eSIM stakeholders are approaching security and compliance. There are signs they are taking a positive approach. For example, 29 per cent see compliance as a driver which can attract customers and build brand trust.

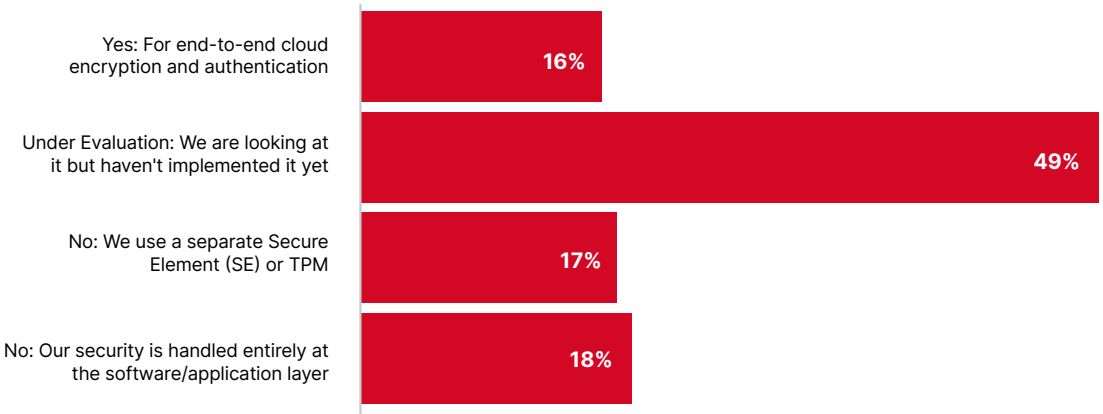
What is your biggest security concern?

eSIM should reduce friction in most connectivity use cases. But does that convenience introduce new security threats? Our study dug into the main concerns. Two key areas were each identified by 33 per cent of participants. The first is the expanded attack surface created by remote provisioning and profile lifecycles including downloads, activations and switching. The second? The increased challenge of governance and access control, specifically regarding roles, audits and the separation of duties across various partners. Supply-chain compromise was cited by 30 per cent. They are concerned by the added risk during eUICC handling, key injection and factory processes.



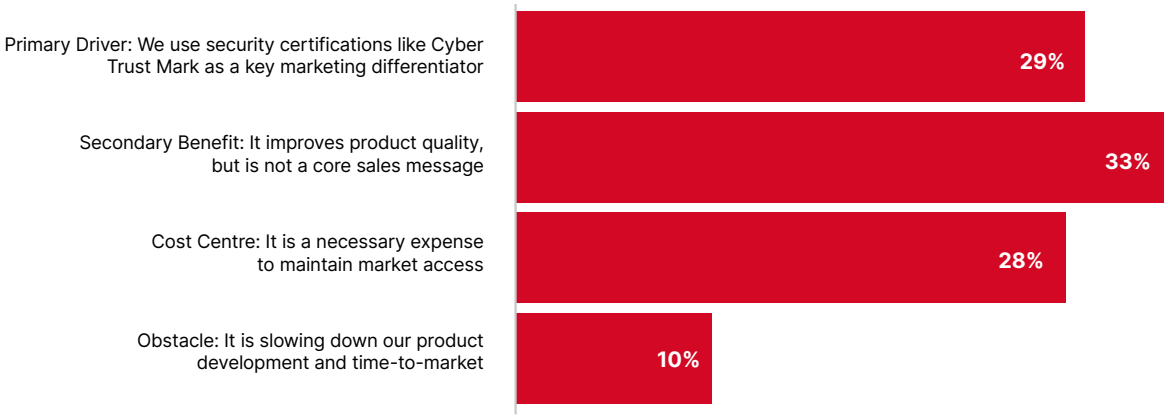
Do you plan to use the eSIM as a Hardware Root of Trust (IoT SAFE)?

The GSMA's IoT SAFE standard was launched in 2021 to give stakeholders a standardised hardware-based root-of-trust. The survey suggests that the standard has been implemented successfully by a minority of respondents. Only 16 per cent say they plan to use the eSIM as a Hardware Root of Trust for end-to-end cloud encryption and authentication. Easily the biggest group (49 per cent) are evaluating IoT SAFE and are yet to move forward with implementation. 35 per cent are not considering a Hardware Root of Trust for the moment. 17 per cent plan to stick with a separate Secure Element or Trusted Platform Module (TPM), while 18 per cent intend to manage their security at the software or application layer.



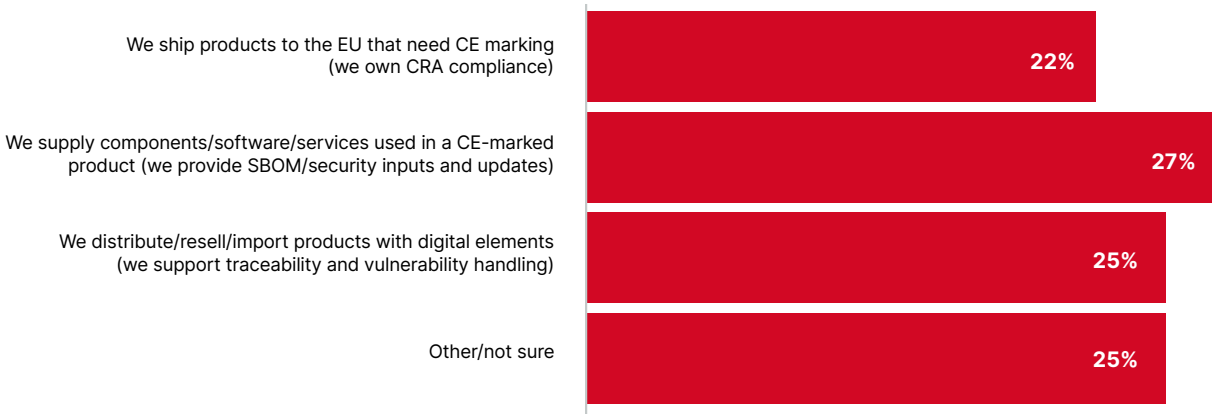
To what extent does cybersecurity compliance drive business growth?

Cybersecurity compliance is inevitable. So, what is the best way to approach it? Should it be viewed as a cost and a hindrance, or a proactive tool for market advantage? 29 per cent of those in the eSIM space are positive. They see compliance as a driver and view high-level security certifications including the US Cyber Trust Mark as differentiators which can attract customers and build brand trust. 33 per cent view compliance as a secondary benefit which will boost product integrity rather than direct differentiation in the market. 28 per cent consider it a necessary expense to operate as a market player. On the flip side, 10 per cent regard compliance as an outright obstacle, hampering product development and increasing time-to-market.



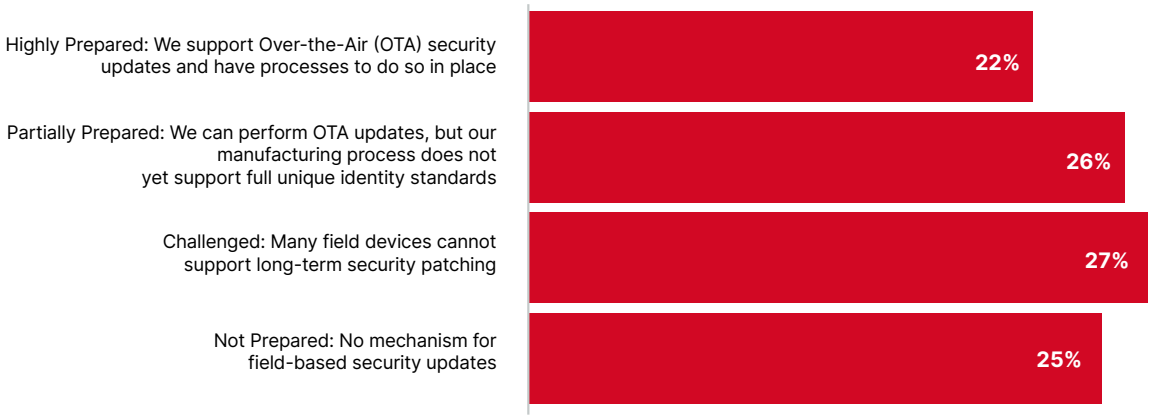
Which best describes how the EU Cyber Resilience Act (CRA) applies to your organisation?

The EU frequently sets the precedent for tech regulation. Cybersecurity is a case in point. Its CRA establishes mandatory cybersecurity standards and will fully apply for those who ship products directly within the bloc. Its scope will include hardware and software vendors, along with distributors of products and enabling services destined for EU markets. So, how will the CRA affect the survey respondents? 27 per cent say it will impact them because they are suppliers of components, software or services used in Conformité Européene (CE-marked) products. 25 per cent expect CRA to affect how they distribute, resell, or import products. Another 22 per cent say they will be impacted because they ship products to the EU which require a CE mark. A final 25 per cent are not sure how the act might apply to them.



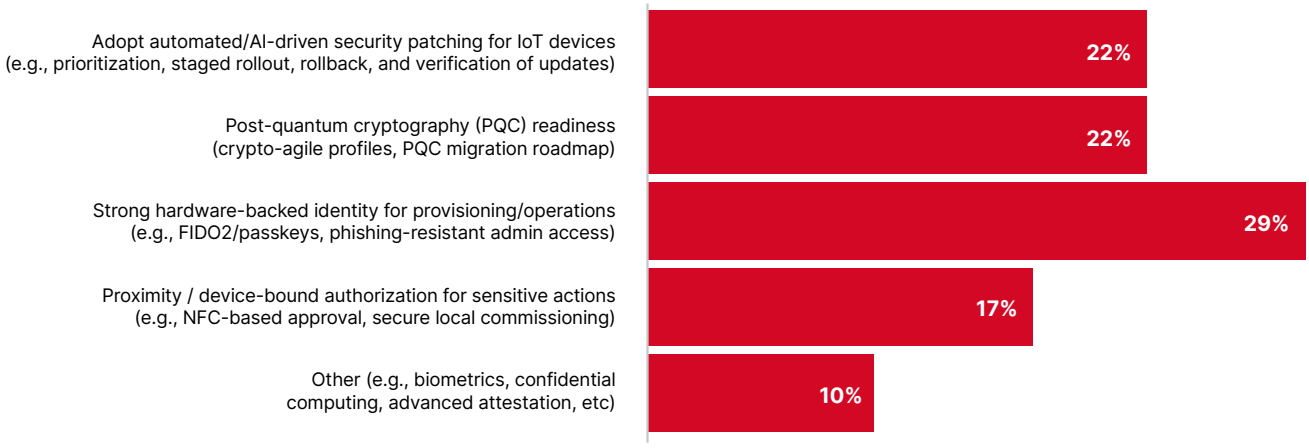
How prepared are you to maintain security updates for five and more years (as required by the EU CRA and USA EO 14028)?

The CRA and US Executive Order 14028 mandate organisations maintain security updates for a minimum of five years. Are respondents ready? It is a mixed story. A respectable 22 per cent of eSIM stakeholders claim to be highly prepared, with the ability to support OTA security updates and the established processes to maintain them. 26 per cent are partly prepared, having the technical capability to perform OTA updates, but requiring updates to manufacturing processes to ensure full compliance. 27 per cent are challenged. Many of their field devices lack the memory and processing power to handle five years of security patches. The SGP.32 standard addresses this challenge and makes cybersecurity compliance simpler. Yet the market needs further education on meeting its compliance needs. The remaining 25 per cent of respondents confess they are not prepared. They have no capability to update devices with the necessary security.



Which next-generation security capability is your organisation most likely to require for eSIMs in the next 24 to 36 months?

In the cybersecurity world, the nature of the threats keeps evolving. As a result, organisations are faced with a constant stream of defensive technologies to choose from. So, which next generation security capability are respondents expecting to require for eSIMs in the coming years? Our survey revealed the most popular choice (but not by much) to be hardware-backed password-less, hardware-backed login methods which provide phishing-resistant access for administrators managing sensitive provisioning systems. 29 per cent selected this capability. 22 per cent are most likely to require automated or AI-driven security patching for IoT devices. The same percentage are considering post-quantum cryptography (PQC) readiness in eSIMs. A slightly lesser number, 17 per cent, say they will need proximity or device-bound authorisation for sensitive actions, such as NFC-based approval. A further 10 per cent cite advanced biometrics, confidential computing, attestation and other capabilities to be useful for their IoT eSIM use.



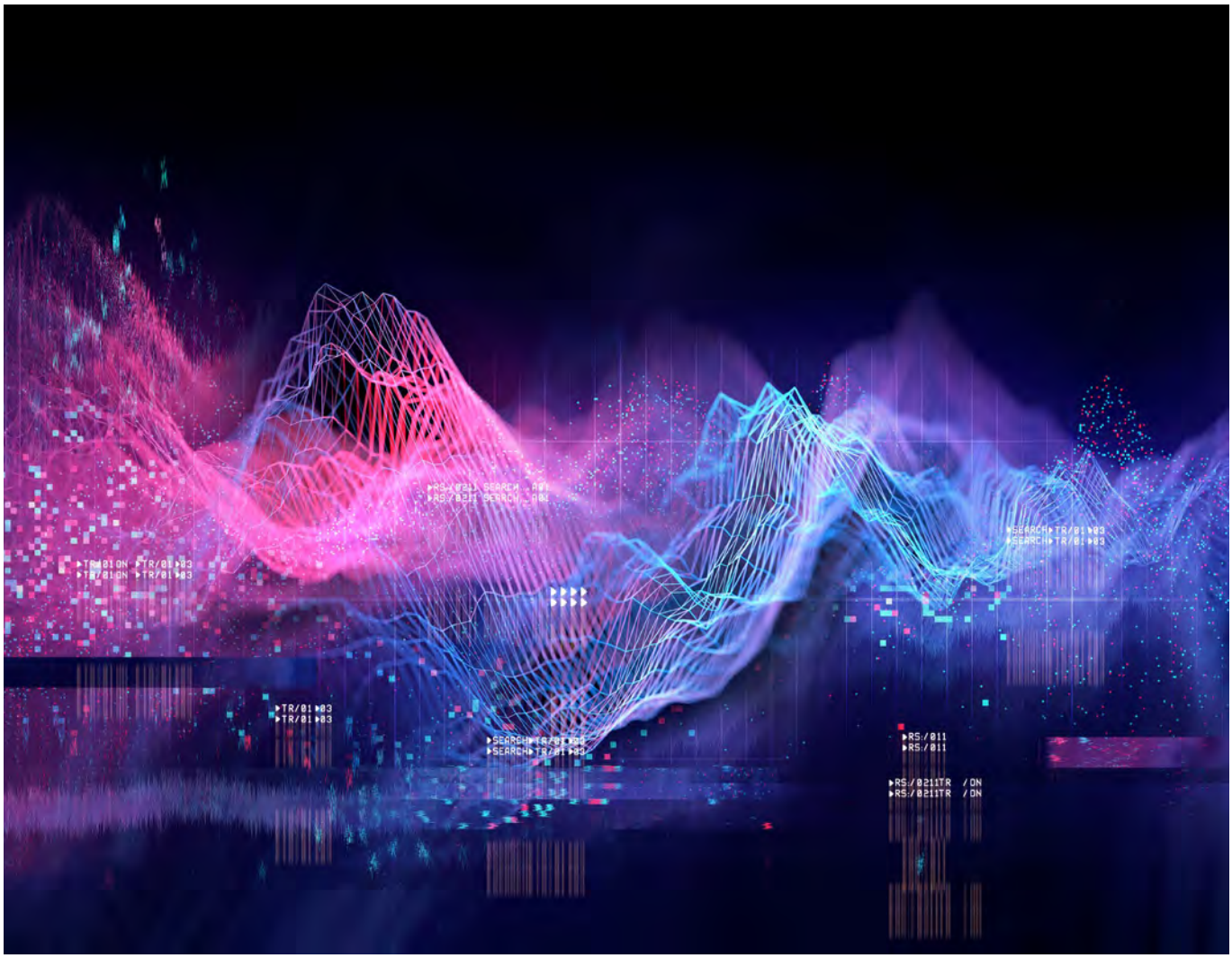
Kigen

Sponsor comment:

The survey captures a clear shift in market thinking: IoT security is becoming a strategic enabler of connected business, not simply a technical safeguard. Enterprises are broadening their focus from device-level protection alone to the wider security of remote provisioning, operational control and lifecycle governance. At the same time, cybersecurity compliance is increasingly recognised for its role in strengthening product quality, supporting customer confidence and creating competitive advantage.

The implications are significant. As new cybersecurity expectations take shape, the organisations best positioned to lead will be those which translate intent into operational readiness, particularly in long-term update strategies, trusted remote management and end-to-end security architecture. The growing interest in advanced capabilities such as IoT SAFE, PQC and AI-enabled remote updates is an encouraging sign for a market preparing for a more resilient future.

This aligns strongly with Kigen's vision that IoT cybersecurity should be simple, scalable and built in from the outset. Our IoT eSIMs, certified to SGP.32, achieve a world-first by delivering automated security patches for CRA compliance. In a world where AI increasingly depends on trusted operational data, secure connected infrastructure will be fundamental to how businesses understand, automate and improve real-world performance.



MOBILE WORLD LIVE

Mobile World Live is the premier destination for news, insight and intelligence for the global mobile industry. Armed with a dedicated team of experienced reporters from around the world, we are the industry's most trusted media outlet for breaking news, special features, investigative reporting, and expert analysis of today's biggest stories.

We are firmly committed to delivering accurate, quality journalism to our readers through news articles, video broadcasts, live and digital events, and more. Our engaged audience of mobile, tech and telecom professionals, including C-suite executives, business decision makers and influencers depend on the unrivalled content and analysis Mobile World Live provides to make informed business decisions every day.

Since 2016, Mobile World Live has also had a team of in-house media and marketing experts who work directly with our brand partners to produce bespoke content and deliver it to our audience in strategic yet innovative ways. Our portfolio of custom work - including whitepapers, webinars, live studio interviews, case studies, industry surveys and more – leverage the same level of industry knowledge and perspective that propels our newsroom.

Mobile World Live is published by, but editorially independent from, the GSMA, producing Show Daily publications for all GSMA events and Mobile World Live TV – the award-winning broadcast service of Mobile World Congress and home to GSMA event keynote presentations.

Find out more at www.mobileworldlive.com