SUMMITAI

WHITE PAPER

ITSM Risks into Growth Opportunities in 2026



How to Turn ITSM Risks into Growth Opportunities in 2026

The IT service management (ITSM) community is currently awash with opportunities to leverage artificial intelligence (AI) to improve IT operations, services, experiences, and business outcomes. However, while the IT world focuses on the possibilities of AI, it's essential that IT leaders don't overlook the many risks in ITSM that may or may not be associated with AI's adoption.

Instead, there's a need first to understand the potential risks (your organization will face in the year ahead) and second to address them, maybe even turning the ITSM risks into business growth opportunities for 2026. So, which risks should you and your fellow ITSM leaders focus on in 2026?

In late Q3 2025, we asked 17 ITSM authorities to answer the question, "What's one risk ITSM leaders are underestimating going into 2026?" with the opportunity to provide actions that will help to mitigate the risks to better place your IT organization and business for growth opportunities in 2026. This crowdsourced paper shares the contributors' opinions, categorized into four areas.

The biggest ITSM risks for 2026

While each ITSM industry authority has their own areas of specialism and interest, four common groupings were identified in their responses.

This grouping might seem a little obvious or even clichéd, but these are:

1. People
2. Processes
3. Technology
4. Value

There are likely other ways to organize the 17 received responses, but this categorization seemed very in line with traditional ITSM thinking.

For example, based on the individual responses, there's really only one technology that ITSM professionals are currently focused on, and that's AI and its potential to enhance IT service delivery and support (and broader business outcomes). Rather than having an "AI" section, the use of "Technology" is preferred for this paper.

The biggest ITSM risks for 2026 in more detail

The following responses were received from the 17 ITSM industry authorities. Each has been lightly edited and, in some instances (where over 600 words were provided), abridged.

1. People

I see two risks, but they're directly related – 'Out of the frying pan' and 'Into the fire.'

Staying in the frying pan: If you don't change your mindset and culture (to Tier-One), you are cooked.

Where Tier-One IT leaders:

- Upend the traditional understanding of the purpose of ITSM, particularly the service desk.
- Are DEX-centric, embracing AI and automation, and seeking to eliminate all possible future incidents before they happen.
- Prioritize personal productivity over service delivery.
- Say: 'AI and Automation mean that the service desk no longer receives or resolves incidents. We don't do that anymore.'

While Tier-Two IT leaders:

- Use traditional approaches that only pass work on to others or back to the employee.
- Embrace current tooling and new AI features.
- Say: 'AI and automation mean my service desk team does the same job faster. Employees can find advice on how to fix issues themselves more easily.'

Jumping into the fire: The proliferation of uncontrolled, hacked, and shadowy AI tools.

The only way to avoid being cooked or burnt is to move out of the frying pan – by becoming a Tier-One IT leader



IAN AITCHISON

Independent Consultant and Advisor

When digital leaders discuss risks entering 2026, the conversation typically revolves around outages, cyber threats, rising costs, tooling, or vendor lock-in. These are important. But they're also predictable. The risk, I believe, we're underestimating is exclusion.

As AI and automation are adopted at pace, organizations face the risk of people being left behind. AI is being embedded into workflows, being used to make knowledge explicit, and decisions are increasingly being shaped by algorithms – often without a deep consideration of the human impact. The danger is subtle: the dashboards stay green, the tickets close, the service level agreements (SLAs) are met – yet people are quietly left behind, falling further and further into the shadows.

As organizations adopt AI and automation, it's important to ensure these technologies are inclusive and empower all employees. AI should be implemented with a focus on uplift – built collaboratively with employees, enhancing their abilities and engagement, and creating new opportunities for growth, learning, and innovation. Importantly, exclusion is not a 'soft' issue. It's a socio-economic risk with real-world consequences:

For consumers

AI systems that lack transparency can entrench bias, creating digital barriers that are invisible but deeply felt. This leads to services that technically function but socially fail to meet expectations. Add to that the practical inequities, such as a lack of reliable internet, outdated equipment, or limited digital literacy. The outcome is exclusion by design, not by accident

For employees

rather than feeling enabled by AI, many feel threatened or overwhelmed. Some worry about being replaced, while others worry about their ability to keep up with new tools and expectations. When people feel AI is 'done to them' rather than 'built with them,' engagement plummets.

For the industry

If we fail to build inclusive pathways for education and training, the ITSM workforce of the future will be less diverse, less confident, and less capable of handling the very complexity AI promises to solve.

Exclusion doesn't appear on dashboards. It won't trigger an incident alert or flag in a quarterly report. But its impact is profound: it breaks trust, stifles innovation, and undermines the very foundations of co-created value.

When managed properly, AI can remove barriers, reduce mundane work, and allow employees to focus on higher-value activities. ITSM leaders who confront exclusion head-on won't just reduce risk; they'll create organizations where their people and consumers are truly enabled to thrive.



DAVID BARROW

Interim Director of Consulting, The ITSM People

I believe one of the biggest risks we have for ITSM leaders is the lack of new, upcoming talent who are interested in following a career path in service management or even know that it exists. For example, the curriculum for Computer Science in the United Kingdom does not include service or service management; the focus is purely on tin, wires, and code. We know that this is not an accurate reflection of what exists in the professional working world, but if we're not helping our younger generations to know what options and career paths are available to them, we face a significant staffing risk.

This risk is an aging service management workforce (heading toward the end of their careers), which is further removed from the younger culture and engagement with technology, with no one to carry on the mantle of driving a service and customer-focused, holistic approach to the delivery of technology services (and beyond).

The resolution must involve apprenticeships, STEM (Science, Technology, Engineering, and Mathematics) Ambassadorship, petitioning the government for change, working with local schools and colleges to enrich their career guidance, and supporting opportunities for young people, including coaching and mentoring (for free).



SOPHIE HUSSEY

Director at Lapis Consultancy Services

It seems like the latest shiny new thing is AI; everybody is leaping onto the bandwagon. It seems to be a case of 'Me too… and NOW'! 'Can I download the whole of AI onto my computer, please?' 'Which is the AI key on my keyboard?' And 'Let's install some chatbots to make our customers happy.'

Inevitably, there will be the massive hunt for the 'AI certificates' and off we go… Once again, the risks standing in the way of success are the five key areas of 'The Shiny New Thing that Really Helps' (Strategic fit, Leadership, Culture, Skills, and Continual learning and improving).

Which, according to my 2024/2025 combined global survey results, has become 'The Rusty Old Thing That We Continually Ignore'! (As we have done with the adoption of the vast majority of other 'Shiny New Things' – such as agile, DevOps, SAFe, IT4IT, ITIL 4, XLAs, and Humanizing IT. Thinking that we can sheep-dip-certify everybody and immediately reap the shiny benefits.

A recent MIT study revealed that 95% of AI initiatives are failing. The primary reasons seem to be choosing the wrong problems to solve (Strategic fit), challenges of measuring AI's impact on outcomes (Strategic fit), the 'learning gap' (Skills) and the lack of learning and adapting (Continual learning and improving), and failure to empower line managers (Leadership).

95%

A recent MIT study revealed that 95% of AI initiatives are failing.

Another MIT study revealed that AI is damaging our critical thinking skills. In contrast, the World Economic Forum's list of key skills in 2030 includes analytical and critical thinking. The World Economic Forum's list emphasizes the importance of soft skills. 'Leadership and social influence,' 'creative thinking,' ' resilience, flexibility, and agility,' and 'empathy and active listening' – Oh dear. These sound somewhat like the ABC (Attitude, Behavior, and Culture) skills. But nobody wants to hear about ABC; it is old (20+ years).

'Haven't you got anything shiny and new instead of ABC?



PAUL WILKINSON

Chief Architect – The Shiny New Thing That Helps

As we head into 2026, the real risk for ITSM leaders isn't technology – it's people. AI and automation are exciting, but service excellence still depends on the skills, confidence, and growth of the service desk. If we overlook this, even the best technology strategies won't deliver what the business really needs.

The service desk isn't just the front door to IT – it's where future managers, architects, and leaders take their first steps. But without structured development in **both** technical and soft skills, careers stall before they've even begun. An analyst who can resolve an incident but struggles to explain it, empathize with a frustrated end-user, or connect the dots to business impact is being set up to fail. In the short term, that leads to unhappy customers; in the long term, it leaves us with potential ITSM and IT leadership gaps.

That's why capability development has to be more than a box-ticking exercise – it's a strategic investment for the future. When we invest in training, build skills matrices, and help analysts understand the business they serve, we don't just improve today's support experience. We retain great people, reduce attrition, and preserve the knowledge that makes organizations strong. The truth is simple: invest in service desk skills today, and you invest in tomorrow's IT leadership.



STEVE CAVE

Principal Associate Consultant - Barclay Rae Consulting

For me, the biggest risk ITSM leaders can face is failing to change. I don't mean the usual 'This is how we've always done it' mindset. Instead, it's ensuring that ITSM leaders fully understand what IT service delivery and support will look like in the next half a decade. This includes the adoption of AI, rising to the challenge of delivering better experiences, and valuing outcomes over operations. Ultimately, if your corporate IT organization can survive without changing (and significantly), I'd question whether the organization as a whole will survive.

Most modern businesses need their technology to work for them rather than against them. ITSM can play a significant role in this. However, simply following ITSM practices isn't enough. Instead, there's a need to provide the IT service delivery and support capabilities that are needed. It's business (and employee)-centric service management rather than IT-centric service management.

The biggest change has to be how ITSM leaders think about what they and their teams do (or, more importantly, what they achieve). While this need encompasses processes and technology, it begins with people and the necessity to rethink IT service delivery and support. It's a revised mindset that focuses on experiences and outcomes, employing technology to make improvements for those who receive and deliver services.



STEPHEN MANN

Principal Analyst and Content Director, ITSM.tools

2. Processes

For me, the risk is not having a business continuity plan ready to address the VUCA world (economy and politics). For example:

- Are you prepared for a cyber-attack?
- What will you do if AI goes amok?
- How are you keeping up with the various policy changes in your country and others?
- How are you engaging and keeping staff?
- What is your plan if a strategic member of your staff becomes ill?
- What is your strategy for obtaining customer feedback on a real-time basis?

If you cannot answer these questions daily, and link the responses to a rolling quarterly plan, you will likely be out of business by 2030. The digital economy won't wait for you to adapt. Your staff and customers will leave.

I recommend using a combination of Value Stream Management and Mapping, connected to XLA practices, to provide your organization with the data and internal collaboration needed to remain safe while improving. I also strongly suggest that you consider the stigma within your organization regarding wellbeing and diversity. It is the responsibility of leadership to ensure that your staff and vendor partners work in an inclusive and safe environment.



DANIEL BRESTON

Independent Consultant and Advisor

The whole industry has become preoccupied with AI – for good reason. AI will radically alter the course of ITSM. But like so many industry trends, AI tools will not solve organizations' fundamental problems. The risk is moving boldly ahead without a solid foundation of organizational capabilities.

AI success in IT Operations is intrinsically tied to mastering ITSM basics. 2026 is shaping up to be a defining moment. The world has undergone an exponential upward shift, and skipping ahead without a solid foundation is a risky endeavor. Equally dangerous, though, is continuing to solve yesterday's problems, which leaves the organization dangerously behind.

Nail ITSM basics and do it now. It's IT's moment.



GREG SANKER

Principal Advisory Director, Info-Tech Research Group

Don't underestimate the complexity of stakeholder engagement in when using continual improvement across diverse business functions.

As your organization accelerates its adoption of AI, automation, and agile practices, the pace of change outstrips traditional ITSM engagement models. Many ITSM leaders might also view the continual improvement and implementation of ITSM processes and procedures as a siloed initiative. Assuming that once a process is optimized, it will naturally be adopted across the entire business. However, in reality, different departments will have vastly different working styles, priorities, and levels of digital maturity.

Therefore, without intentional, inclusive stakeholder engagement, your organization's continual improvement efforts risk being misaligned, underutilized, or even resisted, especially when changes impact cross-functional workflows. To help prevent this:

1. **Map stakeholder landscapes early**
   There's a need to identify not just who is impacted, but how they work, what they value, and the constraints they face.

2. **Co-create improvement goals**
   It's important to involve stakeholders in defining what 'better' looks like. This helps build ownership and ensure relevance.

3. **Use service design thinking to understand and align diverse experiences**
   Techniques such as journey mapping and personas will help here.

4. **Communicate in context**
   Ensure that your organization tailors its messaging to each target group's language and priorities. This helps to avoid "one-size-fits-all" communications.

5. **Measure adoption, not just implementation**
   Employ metrics that allow you to track how improvements are being used and adapted in practice, not just whether they were delivered.

SARAH-JAYNE BULLEY
Service Delivery Manager - Ki



One of the biggest risks ITSM leaders are underestimating going into 2026 is the fragility of their existing service ecosystems. The technology landscape is evolving faster than some governance structures, meaning organizations get sub-optimal results when AI-driven services, niche providers, and technical innovations are added into their portfolios.

At the same time, existing ITSM processes and contracts often struggle to adapt to the continual change. Without a deliberate approach to service integration and management (SIAM), the joins between service providers are frequently the weakest point in the service delivery chain, leading to poor ROI and poor experiences.

This risk matters because competitive advantage doesn't depend on the individual capabilities of service providers; it depends on how well capabilities are orchestrated into end-to-end services. A single integration failure can significantly impact the perceived value of an entire transformation program, erode customer trust, or expose an organization to compliance risks. In a world where boards expect IT to prove measurable ROI from technology investments, leaders must view integration as a strategic discipline. To help mitigate this, ITSM leaders must begin incorporating SIAM principles into their IT operating model.

This change doesn't have to mean a full transformation program. However, service ecosystems do need to be designed with agility in mind, with the investment in integration governance (both technical and management systems) and a focus on the end-to-end experience. Understanding the importance of integration as a source of strategic resilience will help ITSM leaders future-proof their service ecosystems for 2026 and beyond.

More guidance is available in the Scopism SIAM Community, including free access to the SIAM Body of Knowledge. Sign up to be one of the first to access our 2025 refresh.



CLAIRE AGUTTER

Director - Scopism

3. Technology

Unauthorized use of AI by employees is becoming an increasing problem for organizational security and integrity. With the rise of cybersecurity incidents seen in 2025 across multiple attack vectors, I see 2026 potentially as a watershed year for AI use, when the risks of using AI in a corporate environment will take center stage. It's, therefore, crucial for organizations to establish related controls and governance to ensure that AI delivers maximum value securely and responsibly.

It will be essential for organizations to establish internal AI governance across all organizational departments, with ITSM and security teams taking the lead. Security will drive governance, and ITSM teams will serve as the service provider and face of IT, responsible for approving change management and provisioning access to authorized software applications and services within the organization.

Managing the potential explosion in AI use also requires consideration of the data utilized by AI for decision-making purposes. If AI is allowed to run on poorly structured or incorrect data, then errors will occur. Putting controls in place to improve data hygiene includes: defining data governance and ownership, standardizing data inputs, automating data quality checks, security controls for scrubbing credentials and sensitive business information, managing bias where AI wrongly prioritizes outcomes, feedback loops to capture if AI-generated responses are accurate, monitoring, and continual improvement using KPIs and dashboards for IT leadership.



DAVID KEEN

Director - CTMS Service Management

Remember Shadow IT? How about Shadow AI? Unless your organization has a well-formulated strategy of dealing with AI, you'd best assume it is being used 'in the shadows.'

Regarding what can be done, prevention is best – this is best achieved by moving fast enough to stay relevant, I guess.

Ultimately, the LLMs used for AI capabilities are just another tool, but their efficacy and sheer velocity are off the charts. Apply the same principles as with all tools, just be faster.



GIL BLINOV

Senior DevOps Engineer - Fairgen

One overlooked risk that persists year after year is the tendency of organizations to treat everything as a project or a product. Projects and/or products reach a certain degree of "doneness" and are marked complete or are shipped. When is the change to having AI embedded in nearly every application 'done'? It isn't.

We're in a new era of work now. That's not a project with a defined end date, and it's certainly not yet complete. We have to be more adaptable, but it goes beyond Agile, in my opinion. We can't keep thinking in terms of a series of steps or progressions; we are in the age when organizational dynamics need to be treated more like fluid dynamics, with ripples, vortices, and eddies that we cannot currently see.

This change matters because we tend to think linearly, and we can no longer remain innovative and competitive if we continue to do so. We need to find better ways of dealing with complexity.

Fortunately, some thinkers have been working on this for a while and have developed ways to help organizations. Whether that is Cynefin® or some other framework or overlay will vary according to your organization's appetite for risk and its need and drive for innovation. Perhaps the very AI that is part of the complexity can help us see patterns we currently miss within the complexity.

We may be in a different era now, a different stage of the digital revolution, but some of the fundamentals remain constant:

- People will tell us what they like and don't like if we ask them.
- Individuals and small groups will move first and will move faster than larger organizations; encourage innovation by allowing these groups to flourish within larger organizations.
- Good communication is more important than ever.
- Gather data and act on what you discover (even when you don't like it).



ROY ATKINSON

CEO - Clifton Butterfield LLC

As we've seen many times before, organizations have added tools and technology to their service management environments, thinking that these things will solve their challenges… only to find that the underlying issues remain unaddressed. We are starting to see it again, as organizations rush to implement AI-enabled solutions without having done the necessary preparation to ensure success.

The enthusiasm for AI-enabled solutions is well-founded, but organizations will realize the greatest value with a structured, well-prepared approach. For example, AI-enabled tools have the potential to enhance service management environments greatly. I strongly believe that introducing AI capabilities into service management environments will be a game-changer for organizations – if done right.

But, in my opinion, many organizations are simply not ready. They lack adequate data quality and data governance. They are relying on their existing service management capabilities without understanding, let alone designing and documenting, the specific outputs and results they need from service management. Many organizations have already invested lots of money and effort into their service management environment, only to realize a fraction of the expected benefits.

But perhaps the riskiest aspect of this rush to implement AI-enabled capabilities is the lack of a solid business case. Without a well-formed business case, many organizations are adopting AI-enabled capabilities without fully understanding the problem to be solved, much less how the organization will benefit.

Many service management initiatives have failed for this same reason: the absence of a solid business case. History may very well be repeating itself.



DOUG TEDDER

Principal - Tedder Consulting

In my opinion, the greatest risk ITSM leaders are overlooking is that what are commonly called 'AI hallucinations' can severely damage the business. That's why feeding AI with curated, trustworthy knowledge is not optimal – it's critical.



ROGER LABELLE

Head of Product, Provance Technologies

4. Value

One risk ITSM leaders are underestimating going into 2026 is over-focusing on frameworks and tools instead of outcomes. Too many teams still serve the process rather than the people, mistaking compliance for progress.

When ITSM is measured only by the number of tickets closed or steps followed, leaders miss the real outcome: did we actually reduce friction, prevent recurrence, and build trust with the business? Ignoring this risk makes ITSM irrelevant in the eyes of executives.

Utilize methods like The Grove Method to keep outcomes front and center. Frame every ITSM initiative around the business value delivered, not just IT activity. Ask: 'What problem did we prevent?' 'What time did we return to the business?' and 'What trust did we earn?'

When leaders shift the conversation from 'process complete' to 'outcome achieved,' ITSM regains its strategic seat at the table.



BOB ROARK

Director – IT Service Delivery, Boulder Valley School District

Beneath the polished surface of ITSM lies a subtle and dangerous risk: people may be cooperating, but not collaborating. This distinction makes all the difference between service management that looks efficient and service management that actually delivers business value.

Many organizations unintentionally stop at cooperation. Each team optimizes its own performance, but the pieces don't connect into seamless value streams. The result? Services that are well-managed on paper, yet misaligned with what the business actually needs.

Several systemic factors combine to create this risk:

- Fragmented KPIs and OKRs
- Middle managers often focus on optimizing their own department
- Individual reward systems
- Process-centric culture.

The absence of collaboration doesn't just slow things down; it also hinders progress. It creates structural barriers to value creation, including:

- That value streams cannot emerge
- Inefficient handoffs
- Strategic misalignment
- Erosion of trust and morale.

The absence of collaboration is not inevitable. Organizations can take concrete steps to mitigate it by:

- Shifting to value-based metrics
- Adopting value stream mapping
- Creating cross-functional governance
- Fostering a culture of collaboration.

The risk of cooperation without collaboration is dangerous because it hides in plain sight. On the dashboards and reports, everything appears to be in good health. SLAs are green, processes are followed, and teams are busy. But without collaboration, organizations remain fragmented, and value streams cannot emerge. While cooperation 'keeps the lights on,' collaboration lights the way forward.



DAVID BILLOUZ
President, OCIRIS Global

Summary and Steps

Your IT organization will likely be focused on improving its business value in 2026, including supporting the need for business growth. This will not only entail undertaking actions that are directly focused on creating additional business value. It should also include mitigating the ITSM risks that might create barriers to progress or even degrade the business value derived from IT operations and innovation.

The risks for ITSM leaders shared in this paper are varied, and importantly, it's likely that not everything will currently be on your organization's radar. Of course, not all the risks will be applicable. However, it's essential to assess whether a potential risk affects your organization before dismissing it.

It's not a coincidence that more of the submitted risks related to people than any other area. The focus of many ITSM leaders and their teams is currently on the successful adoption of AI technology. However, as with most other technological changes, the change extends beyond the technology itself to affect processes and people, necessitating the use of organizational change management (OCM) tools and techniques to help successfully bring about the desired future state.

If you want assistance with turning ITSM risks into business growth opportunities in 2026,
www.summitai.com/