The next 3 years of internal IT: What's changing *and what isn't*

AI, automation, hybrid working, and evolving technology stacks are reshaping the IT function. Here's what internal IT teams should expect over the next three years.

www.quantasi.com

You've probably seen plenty of predictions about what the future of IT ***IS SUPPOSED TO LOOK LIKE.***

A few years ago, we were told cloud computing would transform everything.

Then it was hybrid working.

Today, AI dominates the conversation.

But technology rarely changes the role as quickly as the headlines suggest.

New tools arrive; businesses adopt them at different speeds. Before long they become part of an environment that's already supporting dozens of systems, hundreds of users and a long list of competing priorities.

You can see that happening now.

AI's becoming part of everyday business operations. Automation's becoming easier to implement. Software vendors continue expanding their platforms, while hybrid working keeps influencing decisions around security, access and device management.

At the same time, much of your role feels familiar.

Projects still need delivering. Systems still require attention. The business still expects technology to be reliable, secure and aligned with its goals.

Whether you're leading a team or managing the entire IT function yourself, the next few years are unlikely to be defined by a single breakthrough that changes everything overnight.

A more likely outcome is a steady stream of developments that gradually influence where your time goes, what skills become more valuable and how the IT function supports the wider business.

AI moves from experimentation ***TO OPERATIONAL REALITY***

A couple of years ago, conversations about AI revolved around possibilities.

People were testing tools, sharing examples and trying to work out where the technology might fit. If an experiment failed, little was lost beyond time and curiosity.

Now things feel different.

There's a good chance people across your business are already using AI in some form.

It may be Microsoft Copilot, it may be features embedded into existing software, or it may be tools that individual departments have discovered for themselves.

As use grows, the discussion moves from what the technology can do, towards how it's managed.

Questions around data access, governance and security become more important once AI starts interacting with business information.

A permissions structure that's been left untouched for years suddenly needs another look when AI can surface content from across the organization.

Information that was previously difficult to find becomes easier to access.

The same applies to user behavior.

People are trying to solve problems and work more efficiently.

They aren't necessarily thinking about where information is being processed, how long it is retained or whether the tool they're using has been approved.

Your role becomes more about making sure AI can be used safely and effectively.

People want guidance. Leadership teams want reassurance. The business wants the benefits without introducing unnecessary risk.

Over the next few years, AI will become another part of the technology estate.

It'll need ownership, governance and ongoing management in the same way as any other business-critical platform.

The technology will continue to evolve quickly. Keeping adoption aligned with security, compliance and business objectives may prove to be the bigger task.

The technology stack gets smaller ***BEFORE IT GETS BIGGER***

Over the past decade, adding software became remarkably easy.

A department needed a solution, somebody found a product that solved the problem, and a new subscription was added to the environment.

Those decisions made perfect sense at the time.

A few years later, you find yourself supporting multiple tools that perform similar functions, managing licenses across dozens of vendors, and trying to understand which systems are important to the business.

This is what happens when technology evolves and different requirements emerge at different moments.

The next few years are likely to bring more scrutiny to those environments.

Budgets remain under pressure and software costs continue to rise.

Leadership teams are becoming more interested in understanding what value they're receiving from the platforms they're paying for.

At the same time, core business platforms continue to expand their capabilities.

Features that once needed specialist applications are appearing within products that are already part of your technology stack.

That leads to questions about overlap.

Are all these tools still required?

Are people using them as intended?

Could some of them be replaced without creating operational issues elsewhere?

Here's an opportunity to simplify.

Fewer platforms mean fewer integrations to maintain, fewer suppliers to manage and fewer systems requiring support.

It can also improve visibility by reducing the number of places where data's stored and business processes take place.

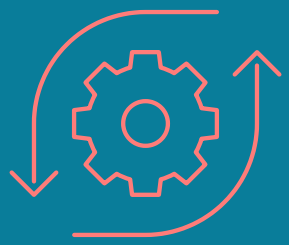
Of course, consolidation isn't always straightforward.

Specialist applications exist for good reasons. Replacing a tool because another platform offers similar functionality doesn't always produce the desired outcome.

It's important to understand which platforms support the way the business operates.

That work takes time, but a simpler environment is usually easier to support, easier to secure and easier to evolve.

Automation ***GROWS UP***



You've probably got processes running today that save time, remove manual work and handle tasks that once required somebody's attention.

Now, automation is becoming far more accessible than it used to be.

A few years ago, many automations were built by technical people solving technical problems.

Today, workflow platforms are being used across departments. Software vendors are embedding automation into their products. And business users are discovering ways to improve processes without needing specialist development skills.

Automation is moving closer to the center of business operations.

Onboarding, approval processes, reporting, compliance activities and countless other workflows can now operate with less manual intervention than they once required.

That creates obvious benefits, but it also introduces a different set of responsibilities.

A workflow that supports a business-critical process eventually becomes part of the environment you're responsible for.

If it stops working, the impact can be every bit as significant as an issue affecting a more traditional application.

That's why conversations about automation are expanding beyond efficiency.

Questions about ownership, documentation and monitoring are more important as extra processes depend on automated workflows.

Understanding who built something, how it works and what happens if it fails becomes more relevant when the automation sits in the middle of an important business process.

Over the next few years, you'll spend less time looking for opportunities to automate and more time deciding how those automations should be managed.

The technology will continue getting easier to use.

Maintaining visibility, oversight and confidence in an environment where automation is becoming part of everyday operations may require more attention.

As adoption grows, the amount of governance surrounding it is likely to grow too.

The skills IT teams rely on ***WILL CONTINUE TO EVOLVE***

Every few years, somebody predicts that a particular technical skill is becoming less relevant.

Then a major outage occurs, a migration runs into trouble, or a security incident demands immediate attention.

The value of that knowledge becomes obvious all over again.

The next three years are unlikely to change that.

Technical expertise remains the foundation of the role.

Understanding infrastructure, security, networking, systems and troubleshooting continues to be as important as it has always been.

The environment may look different than it did ten years ago, but organizations still rely on people who understand how technology works when things don't go to plan.

What's changing is the range of responsibilities around those technical skills.

A growing amount of IT work involves understanding how systems connect, how information moves through the business and how technology supports wider operational goals.

Conversations that begin with a new application or platform can quickly expand into discussions about data, governance, automation, user adoption and business processes.

Technical knowledge becomes more valuable because it provides the context needed to make good decisions across a broader range of subjects.

You likely already spend a significant part of your time translating between ***TECHNICAL REALITIES AND BUSINESS OBJECTIVES.***

That responsibility will become even more important as AI, automation and connected platforms become part of everyday operations.

Developing those broader skills takes time, and that's where you face a challenge.

The day-to-day demands of running the environment continue, while new technologies create fresh opportunities and fresh pressures.

Creating enough capacity for learning, development and strategic work may become as important as the skills themselves.

Hybrid working enters its ***GOVERNING PHASE***

The biggest decisions around hybrid working have already been made.

Whether people spend most of their time in the office, work remotely several days a week, or rarely visit a company location, the model is no longer the center of the discussion.

The focus is consistency.

Once a business accepts that people will work from different locations, questions emerge about how technology, security and governance operate across those environments.

Access to data, device management, user permissions and security controls all become more important when the workforce is distributed.

While the challenges aren't new, what changes is the expectation that they should be managed in a repeatable and predictable way rather than through temporary solutions and workarounds.

The growth of AI adds another layer to the conversation.

A user sitting in the office and a user working remotely may have access to the same tools.

That means policies around data handling, information access and acceptable use need to remain consistent, regardless of location.

Employees expect technology to work wherever they are.

They don't think in terms of networks, office boundaries or security architectures. They expect access to the systems and information required to do their jobs.

Balancing that expectation against security, compliance and operational requirements is one of the more interesting challenges.

Over the next few years, hybrid working is unlikely to generate the same headlines it once did.

The bigger conversation will revolve around governance, consistency and maintaining visibility across an environment that extends beyond the office walls.

The one thing that ***PROBABLY WON'T CHANGE***

When you look back at how IT has evolved over the past ten or fifteen years, the technology has changed enormously.

Platforms have come and gone. Infrastructure has moved. New security challenges have emerged. Cloud services, mobile devices, AI and automation have all altered the way organizations use technology.

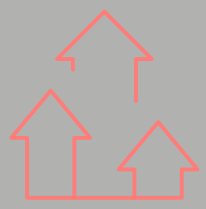
Yet the purpose of the IT function has remained stable throughout all of it.

The business still relies on technology to operate effectively.

People still need systems they can trust.

Leaders still want informed advice when they're making decisions that carry technical, operational or security implications.

Growth still creates new demands on the environment.



Those responsibilities existed before AI arrived and they'll still exist after today's technology trends are replaced by whatever comes next.

New technology can change how work gets done, but it rarely changes why the work exists in the first place.

Over the next three years, you'll almost certainly spend time evaluating new technologies, supporting new ways of working and helping the business adapt to changing expectations.

At the same time, you'll still be helping people solve problems, managing risk, improving reliability and making sure technology supports the organization's goals.

Preparing for evolution ***RATHER THAN REVOLUTION***

If the next three years have a common theme, it's that change will arrive gradually.

AI will become more embedded in everyday operations.

Automation will support a growing number of business processes.

Technology environments will continue evolving as platforms expand, overlap and consolidate.

Expectations around governance, security and visibility will keep growing alongside them.

The fundamentals of your role remain the same.

You'll still be balancing operational responsibilities with longer-term initiatives.

You'll still be making decisions about risk, priorities and investment.

You'll still be looking for ways to support the business while keeping technology secure, reliable and manageable.

The challenge is finding enough capacity to move those initiatives forward while continuing to support everything that's already in place.

That's one reason co-managed support is becoming part of the conversation for more IT directors.

Not as a replacement for internal IT, and not as a transfer of ownership.

It's a practical way to add capacity, access additional expertise when it's needed, and create more space for strategic work, without losing control of your environment.

Success comes from making steady progress, focusing attention where it adds the most value, and ensuring the right support is available when demands begin to outgrow the time and resources available.

A little extra capacity makes a bigger difference than another new technology ever could.

If you're looking ahead to the next few years and wondering how you'll fit AI, automation, governance, projects and day-to-day operations into the same working week, it may be time to consider how additional support could help.

We'd be happy to talk it through.
Get in touch.

EMAIL: sales@quantasi.com
CALL: (574) 217 - 4696