

How to build a 'safe-to-fail' culture for IT teams — and why you should

Removing workers' fear of failure and providing a secure environment for experimentation can clear the path to innovation.



Credit: [Tiger Lily](#)

Companies continue to invest in AI, automation, developer tools, and other new technologies. But [they may not get the results they expect](#) if IT workers don't have the time, resources, or freedom to learn how to use them.

IT workers may be afraid to try new tools if they think a failed experiment could hurt their performance reviews. They may also be unsure which tools and data they can use or how to test new

technology without creating security problems or disrupting the business.

A safe-to-fail culture can help remove those barriers. It gives IT workers room to try new ideas while limiting the risks to the company. Although employees still have to follow rules, they're given the time, approved tools, and secure environments they need to test new ideas. Even if the company decides not to adopt a new technology, it can still learn from the experience.

"To me, a safe-to-fail culture is not a safe-to-be-careless culture," said [Michael Morris](#), global head of platform and talent at Randstad Digital. "It means designing experiments so that a failure is contained, reversible, and useful."

1. Make experimentation part of the job

"Fear of failure is a major barrier, especially when people believe every experiment will be measured against short-term productivity," said Daniel Burrus, founder and CEO at Burrus Research. "Leaders need to separate experimentation from day-to-day performance reviews and give teams permission to test ideas without career risk."

One way IT leaders can encourage experimentation is to set aside time for employees to do it during the workday. If it becomes one more task added to an already busy schedule, workers may put it off or have to do it on their own time.

Typeform, an AI engagement platform vendor, gives employees time during the workday to try AI and other new technologies, said [Aleks Bass](#), the company's chief product and technology officer. Each employee also receives \$1,000 for training, certifications, specialized tools, or other resources that can help

them in their job.

That flexibility is important, because employees in different roles may need different tools and training, she said. Typeform provides some tools to everyone, while the individual budget lets workers try other tools the company hasn't yet approved for wider use.

"So if we're telling people that we want them to experiment with AI ... but we're saying, 'Oh, do that in your own time, with your own money, or your own personal accounts,' then you haven't really created that safe environment to experiment," Bass said.

Morris from Randstad Digital said each experiment should focus on a specific business problem and have a clear goal. For example, rather than simply telling employees to learn AI, managers could ask them to find out whether it can speed up writing test cases, improve technical documents, or automate routine support tasks.

"The key word is 'disciplined,'" he said. "Every pilot should have a business owner, a clear hypothesis, a measurable outcome, a time limit, and an explicit decision at the end: scale it, revise it, or stop it."

Leaders also need to recognize what employees learn, not just what they successfully deploy, Morris said.

"Small, disciplined pilots expose integration, security, quality, and adoption problems while they are still inexpensive to fix," he said. "They also reveal where AI performs well and where human judgment is still required. That allows leaders to redesign the process around the technology rather than simply bolt a new tool onto an old workflow."

One barrier to experimentation is the stigma attached to stopping a project, said [Jeremy Koppen](#), chief information security officer at Equifax.

“To change this, my leadership team and I actively commend our people for shutting down projects that no longer make sense,” he said. “When we go out of our way to appreciate a team for bringing that to our attention, it shifts the dynamic. People know we value their transparency, and they quickly realize they just freed up their talent to do work that actually matters.”

2. Replace uncertainty with clear boundaries

IT workers may also avoid trying new tools because they aren’t sure what the company allows or how much risk it is willing to accept, said [Dom Profico](#), CTO at digital consultancy Bridgenext.

Creating a safe-to-fail culture starts with training employees and ensuring they know what they can and can’t do, he said. As new AI tools emerge, employees need to understand the company’s rules and whether a new tool can do something its existing technology can’t.

Those conversations can keep companies from chasing every new “shiny penny” while still encouraging employees to share ideas that could be useful, Profico said.

Organizations should clearly explain the security and operational rules employees need to follow and put safeguards in place to keep mistakes from affecting customers or users, he said. Knowing those protections are in place may make employees more comfortable trying new things.

Companies can't eliminate every risk, Profico said. If they want employees to try new ideas, they have to give them some freedom, accept that things may go wrong, and apply company policies consistently.

"If you want to run an innovative organization, you've got to really give a little bit more freedom and accept some of that risk," he said.

[Ravi Soin](#), CIO and CISO at Smartsheet, described the approach as creating a culture of "yes, but safely."

IT leaders have to let workers know which systems they can access, how they can use company data, and when they need to involve IT or security, according to Soin.

"Within those boundaries, people should be able to try new technologies without having to go back to IT or security for permission every time," he said.

For example, Smartsheet lets employees in different departments pursue citizen-development projects in preapproved sandboxes.

"If someone in sales wants to use Claude Code for a customer demo, they can do so in a pre-approved sandbox with DLP [data loss prevention] and access controls already configured," Soin said. "So instead of waiting on a security review, they can start the same day."

3. Limit the potential damage

The safeguards should depend on how much damage a mistake could cause, said [Arthur Hu](#), Lenovo's global CIO and CTO of its Solutions & Services Group. An employee testing an AI coding tool, for example, doesn't need as much oversight as an AI agent

working in a critical customer system.

“This starts with analyzing the potential blast radius of a project — meaning the scope of the potential impact to systems and users — and designing the controls accordingly, where a human needs to stay in the loop, what the audit trail needs to look like, and how quickly you can regain control,” he said.

Randstad’s Morris recommended testing new technologies in stages. Employees could start with approved tools and synthetic or nonsensitive data in a sandbox, then move to a test environment and, finally, a small pilot. Access should be limited to what employees need, and the company should monitor and review the pilot and have a plan to stop it or reverse any changes if something goes wrong.

“Security should be a design constraint from the beginning, not a veto that appears at the end,” Morris said. “Only after the team meets agreed performance and security thresholds should the capability reach production.”

Typeform employees can test tools that haven’t been approved for companywide use in sandboxes with mock company and customer data, Bass said. This lets them see whether a tool could help them without putting customers or the company’s platform at risk.

4. Turn experiments into business results

Testing technology early can uncover problems before a company makes a large investment in it, Lenovo’s Hu said. It can also show whether employees trust the technology and whether it fits into the way they work.

"We built a governed AI sandbox on top of our enterprise AI OS. Teams can pull in a new model, tool, or agent framework, stand up a working prototype, and find out whether it earns its place, all without going near production," he said.

"Things that prove out move onto the enterprise platform and inherit our security, reliability, and compliance controls by default," he added.

Typeform took a different approach when it put a small team in charge of developing Research Flow, a product that uses an AI interviewer to collect detailed customer feedback. The company gave the team access to AI tools, set clear goals, and allowed employees to try new ways of working. The team could also earn bonuses for reaching each of three goals, Bass said.

The team, which started work in December, was asked to build a working prototype by the end of February. Without AI tools, the project would normally have taken nine months to a year, Bass said. The company believed the bonuses were worth it because finishing the product faster meant it could bring it to market quicker and begin generating revenue sooner.

NEWSLETTER

Don't miss a thing

Join the Computerworld First Look mailing list for the latest news, analysis, and insights. Sign up now!