Key contact



Ronan Langford
Partner, Risk Advisory
+41 58 279 9135
rlangford@deloitte.ch

Deloitte.

This publication has been written in general terms and we recommend that you obtain professional advice before acting or refraining from action on any of the contents of this publication. Deloitte AG accepts no liability for any loss occasioned to any person acting or refraining from action as a result of any material in this publication.

Deloitte AG is an affiliate of Deloitte NWE LLP, a member firm of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"). DTTL and each of its member firms are legally separate and independent entities. DTTL and Deloitte NWE LLP do not provide services to clients. Please see www.deloitte.com/ch/about to learn more about our global network of member firms.

Deloitte AG is an audit firm recognised and supervised by the Federal Audit Oversight Authority (FAOA) and the Swiss Financial Market Supervisory Authority (FINMA).

© 2018 Deloitte AG. All rights reserved.

Designed and produced by The Creative Studio at Deloitte, Zurich. J14799





IT Risk Management Automation Pulse Survey

Driving value through automation – are you missing out?



Foreword

Introduction

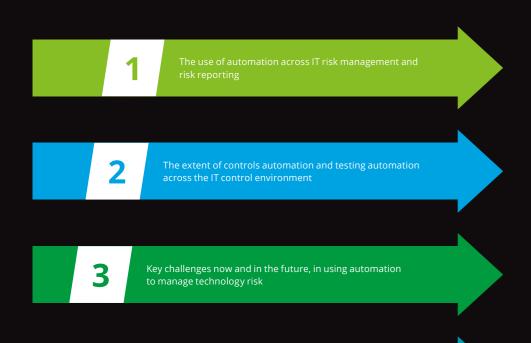
The importance of effective risk management is rapidly increasing in response to the rise in external and internal threats, and the unprecedented wave of innovation across industry.

Automation software, Fintech, artificial intelligence, cognitive computing and blockchain are some of the emerging trends that are expected to have a substantial impact on firms of all sizes.

As business processes become more automated, the need for a robust and reliable control environment, and ability to effectively report on the status of that environment, becomes ever more critical.

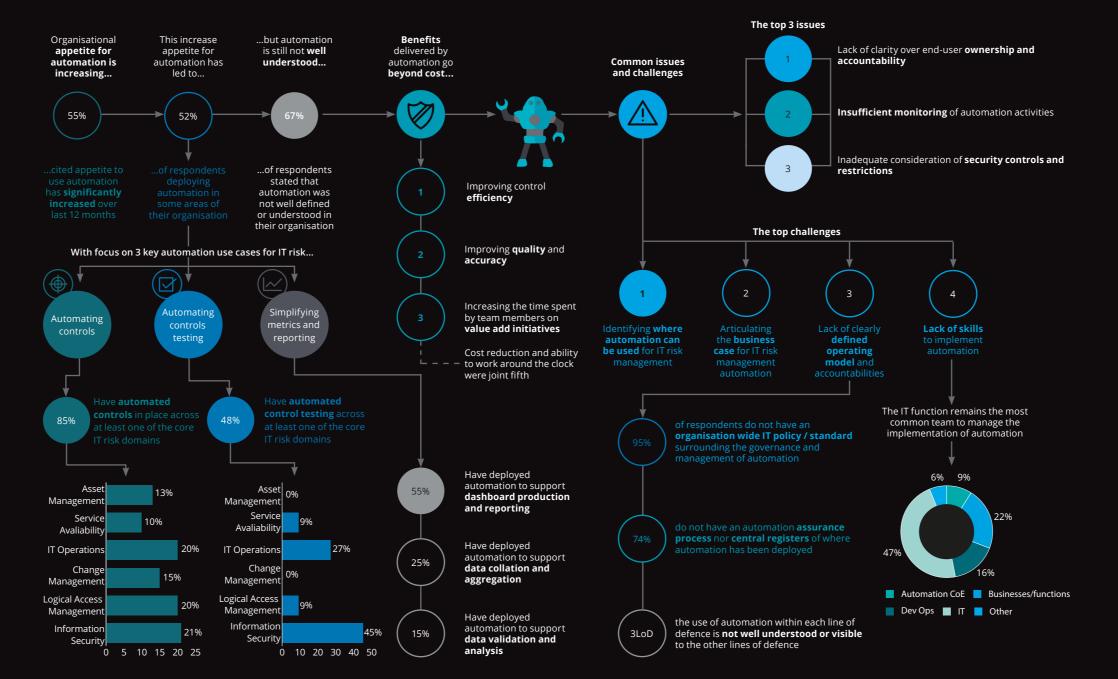
Our objectives

The IT Risk Management automation pulse survey was designed to gather views of professionals in Technology, IT Risk and IT Internal Audit functions across EMEA and across different industry sectors, and capture a cross-industry snapshot of the following:



Key opportunities for the use of automation and cognitive technologies in technology risk management

Findings



Practical steps



Rationalise the control environment and look for opportunities

Delayer and simplify the IT control landscape, looking for automation opportunities across the following 3 key use cases:









Review and refresh the IT risk framework

Review and refresh the existing IT risk management framework, including the change management methodology, to adequately govern the deployment and ongoing management of automation.

Future proof the frameworks by considering emerging development methodologies such as agile, as well as future technologies such as intelligent automation, cognitive computing and artificial intelligence.



Define an automation operating mode

Formally define the automation operating model, including roles and responsibilities for the management and deployment of automation. Consider the adoption of new operating model constructs, such as DevOps, and alignment to the wider IT strategy and operating model.



Build a proof of concept and embed rapid feedback loops

Identify a highly manual, repetitive and logic-driven control or report production process, and build a proof of concept (PoC) to demonstrate the value of automation in the chosen use case. Build the PoC in the development environment to reduce risk and expedite the build. Ensure rapid feedback loops are embedded during the PoC development process to learn, iterate and improve as it progresses.



Develop the business case and increase understanding

Demonstrate both the financial and non financial benefits of automation in risk management, and use the proof of concept to support the business case. This will also help improve the understanding of automation amongst key stakeholders and the wider business.



Increase collaboration across the lines of defence

Look for opportunities to share technology solutions and pool data across the lines of defence to achieve the common goal of an effective and robust technology control environment whilst also meeting individual needs.