Lack of effective automation leads to compliance risks and costs

Submitted by: Maillot Jaune Communications
Tuesday, 22 March 2022

48% of respondents claimed that compliance and auditing tasks are only ‘sometimes completed on time’

London, UK – 22nd March 2022: The new Osirium 2022 IT Automation survey has found that almost half (48%) of UK IT managers claim that compliance and auditing tasks are only ‘sometimes’ completed on time, which risks the introduction of risk and potential costs such as late fees.

This comes alongside estimates that those involved in the compliance and audit process are required to spend an average of 16 hours per week on compliance auditing for IT operations on top of core day-to-day tasks. According to the research commissioned by UK-based cybersecurity software vendor, Osirium, 34% of respondents claimed that too much time is spent on compliance and auditing tasks versus 30% feeling that not enough time is spent here.

Of those saying not enough time is being dedicated, 40% said it was because they don’t have enough staff, or the right staff, to complete the tasks - or it’s due to lack of efficiency in their current processes. A third of respondents think their system is too complex and requires too much attention.

This comes at a time when almost a third (30%) of UK IT Managers would leave their role due to burn out, and 25% due to constant stress at work.

Looking at the issue from a sector perspective, the energy (including oil, gas and utilities) industry spends the most time on audit and compliance with 23 hours per week per person involved in the process, while those from Government institutions spend the least, with 11 hours per week per person involved in the process. Unsurprisingly, 67% of those in the energy sector, would like to be able to automate more of their compliance system.

Almost half (49%) of UK IT Managers across all industries believe that automation would improve their compliance processes, 41% think training staff would help, and 33% would hire more staff to improve it. At the same time, Robot Process Automation (RPA) is used by less than half (41%) of organisations for IT automation and 35% said they were not using RPA due to it only having limited applicability.

David Guyatt, Co-Founder and CEO at Osirium, said: “At a time when organisations are struggling to hire tech talent, businesses should be focusing on simplifying processes for their staff. Organisations are wasting too many valuable resources on manual processes which in turn puts the burden on already time pressured staff. There is clearly also a gap in the market for the right kind of automation to increase compliance and audit efficiencies. Osirium Automation can help every aspect of an IT team’s working life and improves several other key areas in business including customer service and security, whilst also reducing risk, effort and costs.”

Access to the full report can be found here.

-ENDS-

Research methodology
This online survey was conducted by Atomik Research among 1001 IT managers in the UK. Their search fieldwork took place on 28 January – 4 February 2022. Atomik Research is an independent creative market research agency that employs MRS-certified researchers and abides to MRS code.

About Osirium Technologies
Osirium Technologies plc (AIM: OSI) is a leading UK-based cybersecurity software vendor delivering Privileged Access Management (PAM), Privileged Endpoint Management (PEM) and Osirium Automation solutions that are uniquely simple to deploy and maintain.

With privileged credentials involved in over 80% of security breaches, customers rely on Osirium PAM's innovative technology to secure their critical infrastructure by controlling 3rd party access, protecting against insider threats, and demonstrating rigorous compliance. Osirium Automation delivers time and cost savings by automating complex, multi-system processes securely, allowing them to be delegated to Help Desk engineers or end-users and to free up specialist IT resources. The Osirium PEM solution balances security and productivity by removing risky local administrator rights from users, while at the same time allowing escalated privileges for specific applications.

Founded in 2008 and with its headquarters in Reading, UK, the Group was admitted to AIM in April 2016.

For more information visit: www.osirium.com

Media contact:
Clare Shephard
clare.shephard@maillot-jaune.co.uk