RES®

REDUCE COMPLIANCE RISK WITH BETTER GOVERNANCE AND SECURITY CONTROLS

Meeting evolving compliance requirements can be one of the most challenging feats for IT organizations. Unlike the self-imposed guidelines of governance or security, compliance is a set of rules or requests that come from outside an organization. A third party imposes requirements and regulations, which — if not followed and then validated — can result in hefty fines, ruined reputations or even criminal charges. For most organizations, having a comprehensive compliance strategy is a necessary evil, and it brings about security and governance policies that IT is responsible for supporting.

COMPLIANCE BECOMES MORE CHALLENGING EVERY DAY

The landscape of the modern workplace is shifting, resulting in challenges around security. Securing content and data is still the priority, but organizations are experiencing more difficulty doing so because data access points have shifted from the static workplace to the mobile workforce. Seeking innovation and productivity, IT must enable the worker, wherever they are and on their choice of device. Where once content and data was easily secured in one location and device, now — due to increased mobility and accessibility — content and data is less easily secured, vulnerable within the hands of careless workers.

Amidst this shifting landscape, organizations face several common challenges:

- Meet new and ever changing compliance regulations
- Balance worker productivity, innovation and security
- Manage access as workers constantly come and go
- Ensure error-prone manual processes are compliant
- Respond to exhaustive internal and external audits

Not only is maintaining compliance continual and time-consuming, but organizations live in fear of being noncompliant, where the consequences are often detrimental — brand image plummets, customers are unhappy, stocks and revenues decline, and organizations are driven into legislative hearings.

RES customers have reduced the time spent on auditing by up to 50%

SIMPLIFY COMPLIANCE WITH RES

RES provides organizations with the people-centric controls they need to maintain compliance with many of today's data security regulations and standards. The risk of a failed compliance audit is mitigated by focusing on the worker and ensuring that automation is in place, first managing data access based on policy to keep workers productive, then being able to prove that necessary processes are in place – not the other way around. This people-centric approach to compliance, makes audits less of a headache, worker productivity and security is maintained, and policies can be enforced.

RES allows you to empower individual app owners as needed by: automating error-prone tasks, opening or restricting access based on identity, creating on-demand reports for auditors or business leadership, reporting on who has access to what, and gathering deployed workspace details such as changes, usage, devices, apps and configuration to identify potential gaps and fulfill auditor requests. Labor-intensive tasks that used to take days or weeks, can be fully automated to reduce the cost of ongoing governance and diminish the burden on IT who must respond to regular audit cycles.

COMMON COMPLIANCE REGULATIONS RES CUSTOMERS FACE:

HIPPA: The Health Insurance Portability and Accountability Act protects confidential healthcare information and ensure consistency across the healthcare industry. RES automates and secures all digital workspaces for hospitals, clinics and other healthcare organization that must comply with HIPPA. Predicting the services clinicians need and delivering context-aware access keeps patient data secure and improves the quality of service that can be delivered to patients. With RES, you can respond quickly to auditor requests with detailed audit trails and reports.

SOX: Complying with Sarbanes-Oxley is a requirement for all publicly-traded companies to protect investors from the possibility of fraudulent accounting activities. RES puts app-level controls in place to make sure workers only have the level of access they need to get their job done — nothing more and nothing less. Provision access based on identity attributes and context to enforce security policies. Audit trails and reporting help prove controls are in place to protect and manage access to critical financial systems.

PCI DSS: The Payment Card Industry Data Security Standard (PCI DSS) is a global standard for credit card security. RES helps any organization that accepts, processes, stores or transmits credit card information maintain a secure environment for the credit card holder. RES ensures data is protected by enabling IT to provision attribute-based access based on policy, certify access levels, and apply granular app-level security rules at the endpoint. Proving compliance controls are in place is made easy with complete audit trails and reporting.

GDPR: The General Data Protection Regulation (GDPR) is a new EU-based regulation that protects the personal data of individuals within the EU. Any organization that deals with the personal data of individuals within the EU — data “controllers” or data “processors” — must be compliant with GDPR, and RES can help. Securing data with audit-ready compliance measures keeps the workforce productive. Identity and access controls are context aware and IT can protect internal workers from inadvertently introducing threats into their environment. Easily meet the May 25, 2018 deadline with our quick time to value.

If you are required to comply with HIPPA, SOX, PCI, GDPR or other data protection regulations, RES could help you ease the process of meeting compliance audits through the enforcement of your governance and security policies. Organizations do not have to sacrifice productivity for compliance or vice-versa. Compliance and productivity can both be maintained. Contact your RES representative or learn more at www.RES.com.

Why RES?

If you are looking to ease the compliance headaches, RES can help. Organizations can be compliant without sacrificing productivity. Resulting benefits will include:

✓ Greater control over access management
✓ Balanced worker security and productivity
✓ Empowered individual app and system owners
✓ Streamlined audit reporting
✓ Reduced risk of non-compliance
✓ Enforced governance policies

ABOUT RES

RES creates, automates and secures digital workspaces to improve the experience and productivity of the workforce while lowering IT costs. RES takes a people-centric approach to making technology access secure, even in complex multi-device/multi-location scenarios, across physical, virtual and cloud environments. RES boasts numerous patented technologies, fast time to value, and superior customer support for more than 2,500 companies around the world. For more information, visit www.res.com, contact your preferred RES partner, or follow updates on Twitter @ressoftware.