Kaseya®

Automation Cheat Sheet

IT Compliance, Audits and Security

Spend less time on routine IT compliance maintenance, lose less sleep worrying about security, and even learn to love an audit.

Compliance and security issues keep banking and credit union IT professionals up at night. And for good reason. Security breaches and instances of non-compliance can lead to fines and a loss of customer confidence.

Happily there is a better way – and you don't need a Big Bank IT budget to implement it. Today's IT management systems can deliver automation that goes beyond simple tasks that save some time here and there (as important as that is) toward a powerful platform that enables automation of any IT management process you can think of.

This comprehensive cheat sheet outlines all the processes you should be automating right now at your regional bank or credit union.

Process to Automate	Before Automation	After Automation
Compliance		
Discovery	Manual discovery is time-consuming and often fails to discover all devices. Unmonitored devices then fall into non-compliance.	Full, complete, automatic discovery finds all devices on network, including ATMs, branch servers and laptops, self-service kiosks, tablets and other mobile devices.
Non-compliant apps	Non-approved apps aren't detected until they cause issues.	Non-approved apps are found, removed or reported on automatically.
Software deployment	Non-standard deployments may occur because of human error or oversight.	Assure standard and compliant software installations each and every time. Automatically update noncompliant applications.
User privileges and access	Non-standard or non-compliant access or privileges may be granted through human error or oversight.	Privileges and access to data and systems are based on company and compliance policies and applied in a standard fashion.
Audits		
Ongoing monitoring	Manually checking devices and systems is time-consuming and subject to human error.	Operational details, system diagnostics, and all IT activities are gathered regularly and routinely.
Activity logging	Not all activities are logged at the time of service, creating hours of catch-up work prior to an audit.	All activities – whether performed by a technician, helpdesk personnel, or automatically by the IT management system - are tracked and recorded.
Monitoring off-site and off-network systems	Off-site and off-network devices fall out of compliance since there is often no time to go to remote locations.	All devices are monitored whether they are in the office, at a remote branch location, or with an employee at home or on the road.
Reporting	Audit reports are produced after laborious manual system updates.	Reports are quickly and easily produced, and are always up-to-date.

Process to Automate	Before Automation	After Automation
Security		
Patch management	Systems become out of date because patching is time consuming and it's easy for things to fall through the cracks.	All systems are kept up to date by installing and verifying patches with the push of a button; patches are scheduled during off hours to minimize disruption and maximize productivity.
Password management	Weak password policies increase risk of password-related security breaches.	Risk is mitigated with the automatic expiration and changing of passwords.
Malware scans	Haphazard malware scanning leaves data and systems open to risk.	Antimalware software is always installed and up to date with continual scanning to minimize risks.
Detect unusual user behavior	Stressed IT staff may not detect unusual activity given their focus on firefighting known issues.	Users trying to gain access to areas outside their domain, or unusual activities on systems are caught and reported immediately.

Compliance
Stay in compliance -
no matter which IT regulations
you need to adhere to

Audit
Create real-time,
up-to-date audit reports
at the touch of a button

Security
Enable strong security
and data protection
processes

Looking to go beyond automation?

Read this light-hearted **Day in the Life of a System Administrator**
and find out how to get more done every hour, every day.

Kaseya® is the leading provider of complete IT management solutions for Managed Service Providers and small to midsized businesses. Kaseya allows organizations to efficiently manage and secure IT in order to drive IT service and business success. Offered as both an industry-leading cloud solution and on-premise software, Kaseya solutions empower businesses to command all of IT centrally, manage remote and distributed environments with ease, and automate across IT management functions. Kaseya solutions currently manage over 10 million endpoints worldwide and are in use by customers in a wide variety of industries, including retail, manufacturing, healthcare, education, government, media, technology, finance, and more. Kaseya, headquartered in Dublin, Ireland is privately held with a presence in over 20 countries. To learn more, please visit **www.kaseya.com**

Kaseya®