Kaseya®

eBook

How to Manage IT Risk Like a Big Bank

(without a Big Bank Budget)

Compliance, Audits and Security Management for Community Banks and Credit Unions

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.

The stakes are especially high for community banks and credit unions, which face these complicated and time-consuming challenges without the resources of big financial institutions.

- **More than $1 in every $5 of profit spent on regulatory compliance for community banks****
- **72% of credits unions reported ongoing regulatory compliance challenges***
- **Fewer than 1 in 5 credit unions believe their organizations have a comprehensive risk management program in place***
- **79% of community banks rated having a strong technology infrastructure to protect against cyberattacks as their greatest technology concern*****

*Top Tech Trends for Credit Unions, CDW Financial Services
**3rd annual Community Banking in the 21st Century, Federal Reserve Bank of St. Louis
***2015 Growth Strategy Survey, CDW

Kaseya®

> “Small banks cannot afford to efficiently meet the same regulatory and compliance guidelines laid out for ‘big bank’ problems. We are being forced to pay for all the same compliance as big banks without having ‘big bank’ income.”**

Do These Stories Sound Familiar?

Bob is the manager of IT Ops for Centredale Community Bank.

Before every compliance audit, he leaves his wife and two young daughters to stay in a hotel the weekend before the audit. Bob, joined by his whole team, works 24x7, double-checking systems and updating records to make sure they have the answers – and the proof – the auditors will be looking for.

Dan, a hard-working IT technician, recently left Direct Local Credit Union to pursue his dream of surfing the Big One.

After he left, however, his supervisor realized there was no record of all the bank systems to which Dan had admin rights. In addition, technicians at DLCU have a bad habit of sharing admin passwords when stress is high and time is short. As a result, all admin passwords for all bank systems had to be reset, cutting into precious time for the already overworked IT staff.

Frances is a great branch manager.

But with all the responsibilities she has to juggle, she doesn't feel like she has to power down her laptop every day. Or, in fact, any day. Consequently, patch updates haven't been applied to her laptop for months. And she didn't notice she had a virus till who knows how many days had passed. The already-short-handed IT group had to send Dale to go to Frances' location to 1) clean up the virus; 2) install all the patches and updates; and 3) trace all activity from Frances' laptop to make sure no other bank systems (or customer data) was breached. Can you say 'Fun'?

There is a Better Way

Happily there is a better way – and you don't need a Big Bank IT budget to get the technology that will allow you to spend less time on maintenance, lose less sleep worrying about security, and even learn to love an audit.

This ebook uncovers how the right IT management solution can help you simply and easily:

1. Stay in **compliance** - no matter which regulations you need to adhere to

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

3. Enable strong **security and data protection** processes

Three Keys to More Comfortable

Compliance

Let's take a moment to define what we mean by IT compliance.

At it's most basic, it means that you are doing what you're supposed to be doing. You're following the rules, crossing your 't's and dotting your 'i's.

This is the stuff you do every day, day in and day out. There can be internal compliance standards, and, of course, regulatory compliance standards. Different countries and types of financial organizations have different regulations with which to comply.

For example, U.S. banks must meet regulations set by FDIC, FRB, or OCC. For U.S. credit unions, it's NAFCU.

Believe it or not, the right IT Systems Management solution can help you save time and money while *also* ensuring that your IT assets – including data and devices – stay in compliance across your organization.

Here are the three key capabilities you need:

1. Full Discovery and 360° Visibility
2. Continual Monitoring and Alerts
3. Customizable Automation and Policy-based Configuration

Compliance

Let’s dig a little deeper into each of these capabilities and how they can help.

1 Full Discovery and 360° Visibility

You can’t keep your IT networks in compliance if you can’t see everything on them. Your IT Systems Management system must provide full discovery of all devices on your networks – including ATMs, branch servers and laptops, self-service kiosks, and tablets.

Beyond that, you must have visibility into all your new areas of responsibility, including cloud (IaaS, PaaS, and SaaS) and mobile, as well as all your legacy infrastructure (computers, network, storage, and clients) and applications.

And it must find every device and network connection no matter where it’s located, whether it’s currently in a branch location, at an employee’s home, as well as all the details you need to properly manage it from OSs, patch updates, applications, versioning, etc.

2 Continual Monitoring and Alerts

But, of course, the work doesn’t stop with just Discovery. You need a system that will constantly be checking your devices and network, making sure they’re in compliance.

You don’t have the time to check that all applications running on your systems are company-approved and running to spec. But the right IT system management solution will do that for you. Non-compliant applications can be automatically updated to come back into compliance to improve device performance and remove any potential security issues. If non-approved apps are found, you can be alerted or have those apps removed automatically as well.

And, of course, you need complete control and flexibility to configure and define procedures to work within your IT and corporate practices.

That’s where Automation comes in.

Compliance

Automate! Automate! Automate!

3 Customizable Automation and Policy-based Configuration

In order to trust any solution's automation, you need to be confident that you can configure policies and procedures to match your institution's particular requirements:

- Assign multiple sets of policies to each machine
- Determine which policies are obeyed or ignored if a conflict arises
- Check that each machine assigned one or more policies is in compliance
- Show policy status across the organization on a consolidated dashboard
- Enable manual policy overrides

In addition, by automating monitoring and updates, you don't have to worry about human error, which can be introduced via manual efforts.

The right IT systems management solutions will appropriately standardize and update your entire infrastructure, make sure new users are appropriately set up, and make sure all systems are configured according to your instituion's Standard Operating Procedure.

Enterprise Management Associates Recommendations for IT Compliance and Audit

- ✔ Keep detailed, accurate records
- ✔ Maintain up to date inventory of all assets
- ✔ Document processes (and follow them)
- ✔ Conduct interim reviews
- ✔ Spot checks throughout year
- ✔ Automate! Automate!! Automate!!!

Three Keys to (dare we say) Enjoyable

Audits

During an audit, you need to prove that you've done all the work you were supposed to do to keep IT systems in compliance.

Sounds simple, but if you don't have the right systems in place, you and your team may need to work day and night to update all the records the way the auditors want to see them.

Here are the three keys to easier audits:

1. One single system that is a complete source of truth
2. Automatic tracking and logging of all activities
3. Complete, real-time reporting

"I was using too many dashboards to manage all of our systems. Logging into maybe 5 or 6 different systems to check everything… After switching to Kaseya, I thought it was too good to be true."

Ziya Gunay
IT Specialist, Peoples Bank & Trust

Audits

Let's take a closer look at how to ace an audit.

1 One Single Source of Truth

Using and maintaining multiple point solutions has a cost beyond productivity. Consolidated tracking and reporting becomes difficult and cumbersome. Sure, you can create scripts to export and combine reports from various systems. But you're not in the business of creating integrated IT management solutions – and your scarce IT resources shouldn't be squandered this way.

Instead, one system that provides visibility to your entire network translates into one point of truth you can turn to when conducting an audit.

2 Automatic Activity Logging

Whether you and your team update a server automatically (via configured automation policies), remotely (by a technician using endpoint management) or on premise, you need to make sure all activities are automatically logged and recorded.

This information can then be collected and used to populate easy-to-read reports that you can send upstairs to senior management, your own staff, and, of course, auditors. Instead of weeks or months to compile a complete audit, you can have this information on-demand by creating a report.

3 Real-time Reporting

In addition, by tracking all activity and continually monitoring all devices on your network infrastructure, you are guaranteed that your audits and reports are quick, easy and always up-to-date.

This real-time reporting means you can also conduct interim audits to review all procedures and make sure everything is working as intended.

Three Keys to Simplifying Your

Security

Data and infrastructure security is an essential strategic concern that, unfortunately, doesn't have a simple one-size-fits-all solution. But that doesn't mean you can put your head in the sand.

IT systems management systems – priced for regional banks and credit unions – include the capabilities you need to feel confident of your security procedures.

We've already touched on some IT systems management capabilities that are fundamental for robust security, such as complete discovery and auditing, a single, holistic view of system health, and automatic activity logging.

In addition, regional banks and credit unions need:

1. Comprehensive software patching and updating
2. Robust Identity and Access Management (IAM)
3. Alerts on potential security issues that include, but go beyond antivirus and anti-malware

Security

Your first two steps toward a better night's sleep.

1 Comprehensive Software Patches and Updates

Security breaches and performance problems are less likely to crop up in the first place with software updates and security patches done in a routine, timely and dependable timely fashion.

However, ensuring patch and software updates are routinely and completely applied can be difficult. You know by experience that you can't count on users to shut off their machines, download updates, or follow update instructions in any way. But you can't afford to go to each device and conduct manual updates.

You need to be able to automate remote patching and updating including remotely shutting down machines if necessary and intervene only if there's a problem.
Of course, you need to have the ability to base updates on predefined patch policies and schedules that minimize network impact.

2 Robust Indentity and Access Management (IAM)

IAM encompasses many capabilities, including:

- Credential management to centrally organize and control passwords for your team and customers.
- Password automation to force the expiration and changing of passwords
- Password auditing which will ensure you meet compliance obligations and gain visibility into password access.
- Multi-Factor Authentication that increase security by proving the identity of staff as they login from wherever they are.

You should also be able to control access to data and systems by user level as well as policy-based roles.

Security

Stay Alert and Ahead of Potential Problems.

3 Alerts on security and utilization issues.

Antivirus and anti-malware are absolutely required. However, in today's world, they are just table stakes for a robust security plan.

You need to be alerted of any potential security breach beyond viruses and malware, including unusual patterns of user behavior or access, or suspicious spikes in bandwidth utilization.

Automatic detection and alerting of all these incidents (throughout all devices and entire infrastructures) gives administrators a better understanding of the health of their overall IT environment.

In addition, all access can be recorded so that, in the event of an incident, you have all the information you need to identify the sequence of events and the root cause.

Next Steps

Imagine what you and your team could do with the time you'd get back if there were a simple, easy and affordable way to:

- Stay in compliance - no matter which standards or regulations you need to adhere to
- Create real-time, up-to-date audit reports at the touch of a button
- Enable strong security and data protection processes

Kaseya VSA and AuthAnvil can empower your team to spend less time on time-consuming maintenance, lose less sleep worrying about security issues, and maybe even learn to love an audit!

Frankly, you owe it to yourself and your team to take the next step:

Click below for a free trial of Kaseya VSA

Learn how VSA and AuthAnvil work together to provide an added layer of IAM protection to your users and infrastructure.

Contact sales today for a price quote at sales@kaseya.com

Try it!

Take Kaseya VSA for a spin.
Sign up for a free trial.

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**