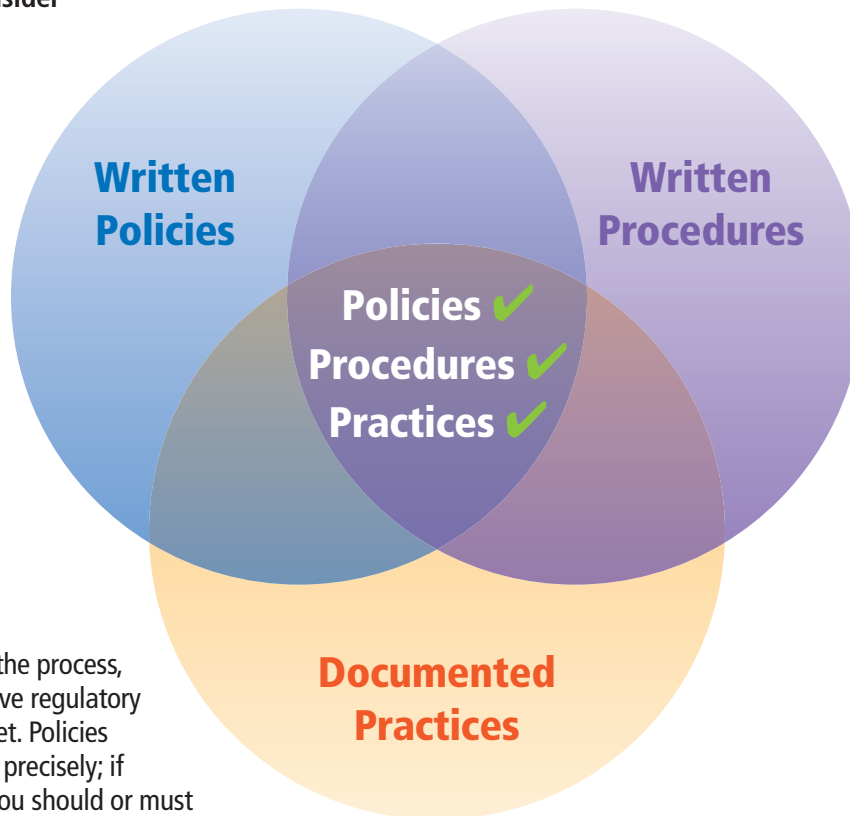


Using Technology to Drive Compliance

Thomas Hinkel, Director of Compliance, Safe Systems, Inc.

In the past year to year and a half, nearly all of the IT examination findings I've seen have in the broad category of "documentation," or more specifically, lack thereof. In other words, policies and procedures were satisfactory, but documentation was either non-existent, or insufficient, to demonstrate that actual practices followed policy and procedure.

To visualize this, consider that the compliance process consists of three overlapping areas of endeavor:



Written polices begin the process, which must always have regulatory guidance as their target. Policies should track guidance precisely; if guidance states that you should or must do something, your policies should state that you do, or you will.

If policies are "what" you do, written procedures are the "how." And just as policies align with guidance, procedures should flow logically from, and align with, your policies. For example, your information security policy states (among other things) that you will protect the privacy and security of customer information. Your procedures contain the detailed steps (or controls) that you will take to prevent, detect and correct unauthorized access to, or use of, customer information. Controls like securing the perimeter of your network, updating server and workstation patches, installing and updating Anti-virus, etc.

So you have the "what" and the "how," but as I mentioned previously, the vast majority of audit and examination findings in the past couple of years were due to deficiencies in the third area; actual (documented) practices. And this is where technology can be of tremendous assistance.

Auditors and examiners much prefer automated systems over manual. Automated systems don't forget, or get too busy, or take vacations or sick days. They aren't subject to human error or inconsistencies. In fact, some processes like firewall logging, normalization, and analysis are virtually impossible to implement manually because of the sheer volume of data generated by these devices.* And while other areas like patch management and Anti-virus updates are possible to implement manually, auditors much prefer automated processes because they ensure policies are applied in a consistent and timely manner.

But perhaps the biggest boost to your compliance efforts from technology is in the area of reporting, and specifically, automated reporting. In today's compliance environment, if you can't prove you're following your procedures, the expectation from the examiners is that you aren't. This is the one area that has evolved more than any other in the past couple years. And automated reporting provides that documentation without human intervention, easing the burden on the network administrator. Auditors (internal and external) and examiners also like automated reporting because they have a higher confidence in the integrity of the data. And the IT Steering Committee likes it because it is much easier to review and approve reports prepared and presented in a standardized format.

So in summary, technology enables automation, and automation enhances compliance. And along the way everyone from the Board of Directors, to management committees, to the network administrator, benefits from it.



About the Author

Tom Hinkel is the Director of Compliance for Safe Systems and is responsible for ensuring that Safe Systems' financial institution clients incorporate and abide by appropriate financial industry regulations and best practices. Hinkel has over twenty five years' experience in IT regulatory compliance and is a certified auditor, published author for several national banking publications, and writer for the compliance helpsite complianceguru.com.

* The FDIC IT Officer's Pre-Examination Questionnaire validates the difficulty of manual processes to manage logs when it asks: *"Do you have a formal intrusion detection program, other than basic logging (emphasis mine), for monitoring host and/or network activity"*

About Safe Systems, Inc.

Founded in 1993, Safe Systems is the national leader in providing compliance-centric IT solutions exclusively to financial institutions. As a technology partner, and recent winner of the BankNews Innovative Solutions Award, Safe Systems has worked with over 500 financial institutions and manages over 20,000 network devices nationwide. Safe Systems' scalable and cost effective solutions include IT managed services, compliance solutions, business continuity and disaster recovery, hosted email, data vaulting, network design and installation, security services, and IT and compliance training. Safe Systems helps financial institutions to significantly decrease costs, increase performance, and improve compliance posture. For additional information, please visit www.safesystems.com or call **877.752.0550**.



About Kaseya

Kaseya is the leading global provider of IT Systems Management software. Kaseya solutions empower virtually everyone — from individual consumers to large corporations and IT service providers — to proactively monitor, manage and control IT assets remotely, easily and efficiently from one integrated Web-based platform.

Go to www.kaseya.com/financial for a **FREE** trial.

Visit: www.kaseya.com | Email: banking@kaseya.com | Like: [Facebook.com/KaseyaFan](https://www.facebook.com/KaseyaFan) | Follow: [@KaseyaCorp](https://twitter.com/KaseyaCorp)

©2012 Kaseya. All rights reserved. Kaseya and the Kaseya logo are among the trademarks or registered trademarks owned by or licensed to Kaseya International Limited. All other marks are the property of their respective owners.

