

Automating Compliance Activities

Dave Millier, Uzado Inc.



What Are We Talking About?

- Collecting of information
- Performing Routine Tasks
- Verification (Managing)
- Validation (Confirming Compliance)

Sample Compliance Activities

- Confirm a meeting took place
- Verify Anti-Virus is installed on all windows desktops and servers
- Confirm there are no "ANY" firewall rules
- Verify new servers have been hardened

Why Automate?

- Save Time
- Save Money
- Avoid Audit Fatigue
- Consistent, Reliable, REPEATABLE Results

Compliance Lifecycle

- Plan your compliance activities
- Implement Your Approach
 - Tools
 - Processes
 - Training
- Ongoing Management
- Perform Periodic Compliance Activities, Measure Results
- Rinse and Repeat

Understand Your Audience

- Who needs to know about your compliance activities
- How will you present your results?
 - Reports
 - Dashboards
 - Evidence
- How will they USE the information you present?
- What frequency do they need it?
- How will you ensure consistency?

Compliance Measurement Process

- Determine what compliance means
- Determine how you will achieve this result
- Create a process to gather appropriate information
- Build a Workflow to Visualize the Process
- Test and Validate the Process Actually Works

Doing It Manually

- Start by performing process manually
- Walk through each step, gather information
- Confirm that the output/results from each step are sufficient to go on to next step
- Tune as required
- Sometimes this is all you need
- Sometimes automation is not an option

Sample Automation Tools

- Puppet
- Chef
- PowerShell
- Shell scripts
- Commercial GRC products

Apply Automation

- Review the Process and Workflow
- Identify which steps may be candidates for automation
- Determine how you would perform the step manually
- Choose the appropriate automation method
- Implement your approach
- Test and validate
- Tune as necessary

Tracking Progress

- How often are you going to validate compliance?
- What are you going to do with the results?
- How will you handle something out of compliance?
- Make sure to tune your processes when necessary

Reports, Dashboards

- Management Reports and Dashboards
- When to dashboard, when to report
- Evidence Reports
- Easy access to information
- Historical information
- Right information, right people, right time

Let's Automate!

- Verify Anti-Virus is installed on all desktops and servers
- Confirm there are no "ANY" firewall rules

Summary

- Compliance management is a process
- You can apply everything we discussed to risk/security management and operations management
- You need to keep doing it
- Don't let people game the system (periodic double checks)
- You can save a lot of time and effort AND get much better results through automation

Questions?

Dave Millier

www.davemillier.com

dmillier@Uzado.com

Uzado Inc.

www.Uzado.com

