

RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: GRC-R03

Surviving SOC2 – The Why and How for Cloud Service Providers

Shaun Gordon

VP & CISO
New Relic, Inc.
shaun@newrelic.com

CHANGE

Challenge today's security thinking



What we'll talk about

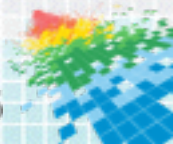
- ◆ What is a SOC2
- ◆ Why you should consider one
- ◆ Why it might not be as scary as you think
- ◆ How to get through the audit
- ◆ Tips & Tricks



Disclaimers



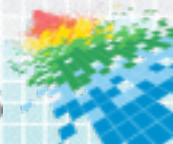
- ◆ Your mileage may vary



Disclaimers



- ◆ Your mileage may vary
- ◆ I am not an auditor



Disclaimers



- ◆ Your mileage may vary
- ◆ I am not an auditor
- ◆ I am not advocating security through compliance



Disclaimers



- ◆ Your mileage may vary
- ◆ I am not an auditor
- ◆ I am not advocating security through compliance
- ◆ All viewpoints expressed are my own and should not be attributed to New Relic



What is SOC2?

- ◆ Focussed on Service Providers vs. Financial Controls
- ◆ Prescriptive vs. Descriptive
- ◆ Built around Trust Service Principles
 - ◆ Security
 - ◆ Availability
 - ◆ Processing Integrity
 - ◆ Confidentiality
 - ◆ Privacy
- ◆ Type I vs. Type II



Why conduct a SOC2 (or why are you here?)

- ◆ Customer request
- ◆ Help with sales process
- ◆ Measure yourself
- ◆ Provide a framework for your security Program



Reasons to be Scared

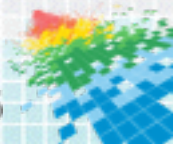


- ◆ Unsure of value
- ◆ Too much work
- ◆ Better to focus on real security than compliance
- ◆ Might fail



Failure?

- ◆ Exceptions are not unexpected
- ◆ ... and they are learning opportunities
- ◆ You are probably under no obligation to share report 1st time around
- ◆ ... and you can provide context when you do share
- ◆ Set expectations with your management



If You're Not Sure

- ◆ Conduct a high-level gap analysis
- ◆ Get Trust Service Principles & Criteria (TSP Section 100)
 - ◆ Illustrative Risks and Controls (Appendix B)

	Criteria	Risks	Illustrative Controls
Criteria Common to All [Security, Availability, Processing Integrity, and Confidentiality] Principles			
CC1.8 Common Criteria Related to Organization and Management			
CC1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and requirements as they relate to (insert the principle(s) being reported on: security, availability, processing integrity, or confidentiality or any combination thereof).	The entity's organizational structure does not provide the necessary information flow to manage [security, availability, processing integrity, or confidentiality] activities.	The entity evaluates its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process and revises these when necessary to help meet changing commitments and requirements.
		The roles and responsibilities of key managers are not sufficiently defined to permit proper oversight, management, and monitoring of [security, availability, processing integrity, or confidentiality] activities.	Roles and responsibilities are defined in written job descriptions and communicated to managers and their supervisors.
			Job descriptions are reviewed by entity management on an annual basis for needed changes and where job duty changes are required necessary changes to these job descriptions are also made.
		Reporting relationships and organizational structure do not permit effective senior management oversight of [security, availability, processing integrity, or confidentiality] activities.	Reporting relationships and organizational structures are reviewed periodically by senior management as part of organizational planning and adjusted as needed.

Rate Yourself



No problem



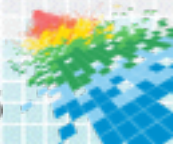
Probably OK (but might need to tweak)



With a little work



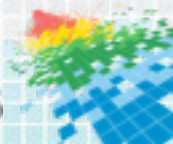
Heavy lift



Get Started

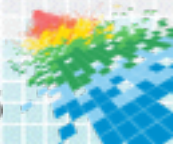


- ◆ Determine scope, area, and type
- ◆ Find an auditor
- ◆ Conduct a gap analysis
- ◆ Start addressing gaps
- ◆ Policies are potentially your long pole



Start Gathering Data

- ◆ Use auditor requests supplemented with Illustrative Risks and Controls
- ◆ Create a repository
- ◆ Helps to identify who will provide what information
- ◆ Helps to avoid surprises and missing data



Welcoming the Auditors

- ◆ Heads-up to company
- ◆ Brief primary contacts
- ◆ Don't forget access & space
- ◆ Your job isn't over when they arrive



Managing the Audit(ors)



- ◆ Play translator
- ◆ You are a special snowflake
- ◆ Auditors might not know agile, devops, etc.
- ◆ Suggest non-traditional controls



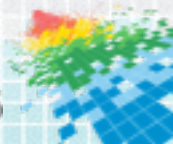
Security Principle 2.5

- ◆ Changes that may affect system security are communicated to management and users who will be affected.
- ◆ Describe how planned changes to system components and the scheduling of those changes are reviewed.
- ◆ Describe how changes to system components, including those that may affect system security, require approval before implementation.



Security Principle 2.5

- ◆ Changes that may affect system security are communicated to management and users who will be affected.
- ◆ Describe how planned changes to system components and the scheduling of those changes are reviewed.
- ◆ Describe how changes to system components, including those that may affect system security, require approval before implementation.



Sidekick Process

- ◆ All changes reviewed by another developer
- ◆ Must add “ship-it” comment to pull request
- ◆ Security team has automatic nightly script to audit for sidekick
- ◆ SOC2 auditors audit sidekick process and nightly script



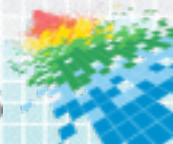
it!



Managing the Audit(ors)



- ◆ Play translator
- ◆ You are a special snowflake
- ◆ Auditors might not know agile, devops, etc.
- ◆ Suggest non-traditional controls
- ◆ Don't take no for an answer



Don't take No for an Answer

- ◆ Missing evidence of actual gap?
 - ◆ Can you find it elsewhere?



Missing Evidence



franky commented on Nov 6, 2014

Owner

Removing an unneeded background job and model with accompanying routes. I'll have a final follow-up PR to drop the table after this goes out.

@mnoble

 `Made all models that access RPM as readonly ...`

 fb5b62a



mnoble commented on Nov 7, 2014



Missing Evidence



franky commented on Nov 6, 2014

Owner

Removing an unneeded background job and model with accompanying routes. I'll have a final follow-up PR to drop the table after this goes out.

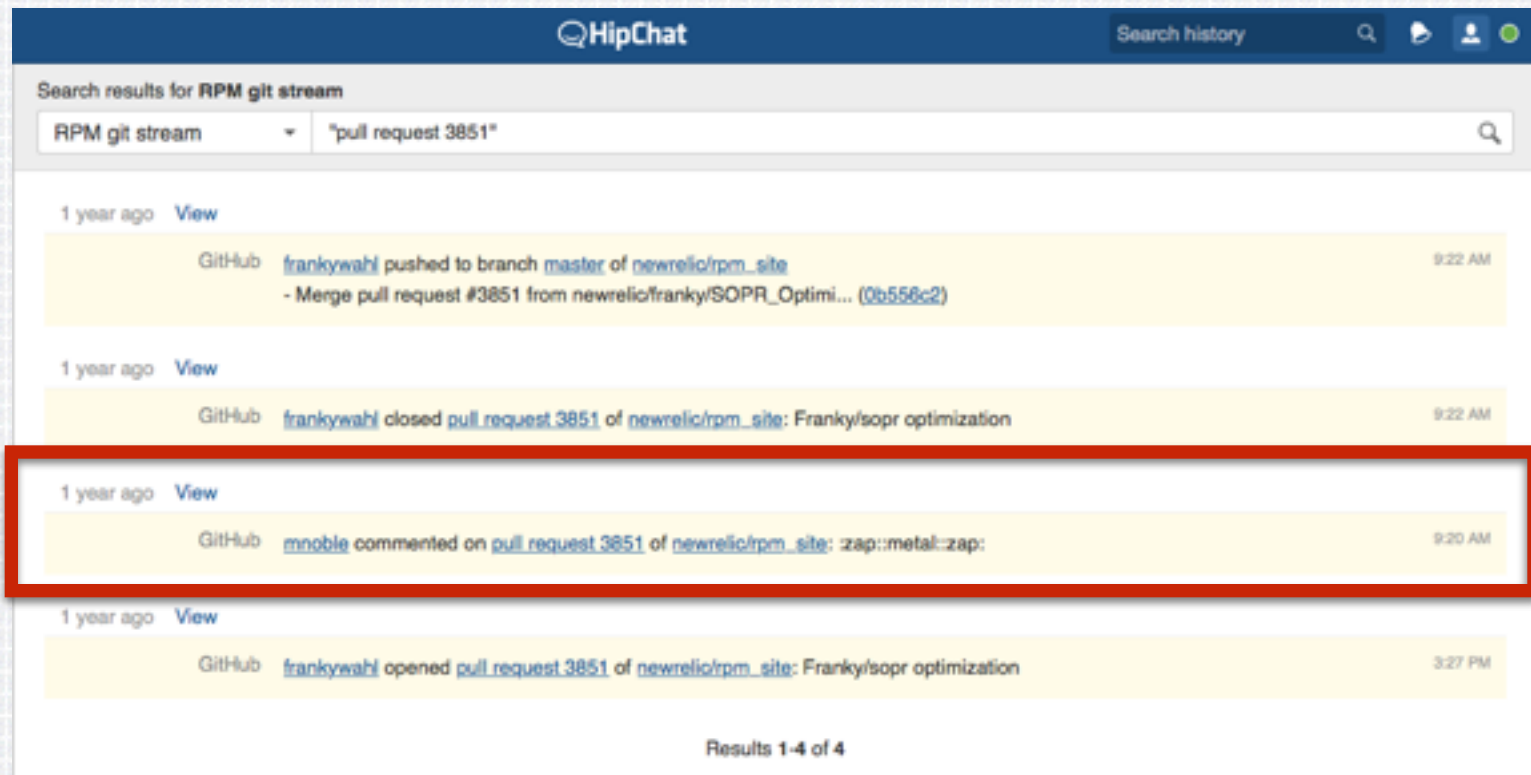
@mnoble

 `Made all models that access RPM as readonly ...`

 fb5b62a



Missing Evidence



HipChat

Search history

Search results for RPM git stream

RPM git stream "pull request 3851"

1 year ago [View](#)

GitHub [frankywahl](#) pushed to branch [master](#) of [newrelic/rpm_site](#) 9:22 AM
- Merge pull request #3851 from newrelic/franky/SOPR_Optimi... (0b558c2)

1 year ago [View](#)

GitHub [frankywahl](#) closed [pull_request.3851](#) of [newrelic/rpm_site](#): Franky/sopr optimization 9:22 AM

1 year ago [View](#)

GitHub [mnoble](#) commented on [pull_request.3851](#) of [newrelic/rpm_site](#): :zap::metal::zap: 9:20 AM

1 year ago [View](#)

GitHub [frankywahl](#) opened [pull_request.3851](#) of [newrelic/rpm_site](#): Franky/sopr optimization 3:27 PM

Results 1-4 of 4

Don't take No for an Answer

- ◆ Missing evidence of actual gap?
 - ◆ Can you find it elsewhere?
- ◆ Are there compensating controls?
 - ◆ You know your environment better than the auditors
- ◆ Beware the “requested evidence” trap
 - ◆ Sometimes you need to back up
 - ◆ Ask which control trying to satisfy
- ◆ ... and keep perspective



Wrap-up

- ◆ Retain documentations and steps to reproduce
- ◆ Get feedback from data providers
- ◆ Review report (findings, informational finding, & sufficient controls)



Rate all Gaps & Sufficient Controls



Passed with flying colors —
Don't worry



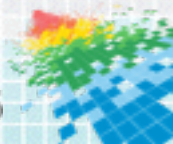
Passed, but controls could
change under you — Educate on
importance or find other controls



Squeaked by — Treat as a
gap

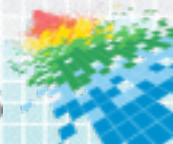


Finding — Fix it or implement a
control



Wrap-up

- ◆ Retain documentations and steps to reproduce
- ◆ Get feedback from data providers
- ◆ Review report (findings, informational finding, & sufficient controls)
- ◆ Create plans... and track
- ◆ Share finding with Sr. Management
 - ◆ Don't waste a good bludgeon
- ◆ Thank people that helped



Your Job Continues



- ◆ Execute on your remediation plan
- ◆ Implement your improvements
- ◆ Don't forget you have 6 months
- ◆ Do a pre-audit
- ◆ Consider increasing scope



Unintended Benefits

- ◆ Wows customers
- ◆ Competitive differentiator
- ◆ Provides structure to security program
- ◆ Ensures a consistent high bar
- ◆ CSA Star self-registry was easy
- ◆ Supports cloud security story



Shaun's Cloud Security Story™

Cloud is not inherently less secure than on-premise.

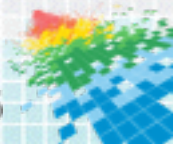


But you need transparency to prove it.



Get Started

- ◆ Understand your business case... will this add value?
- ◆ Conduct high-level gap analysis
- ◆ Decide if you are ready
- ◆ Even if not, start with a self audit



RSA[®]Conference2015

San Francisco | April 20-24 | Moscone Center

Thank You!

shaun@newrelic.com

 #RSAC

