St Louis CMG Meeting

July 17, 2018

# Actionable Intelligence Demands ACTION to Address Business Risk

*Presented to you by:*

*BEN DAVIES*

We make heavy use of the comments section.
Download the presentation for that data.

# Agenda

Change the way you think about doing capacity management and performance management.

- Brief introduction
- Our “Job”
- Action based on Compliance to Policy or Standard (or Make one)
- Business Risk (all that really matters)
- Solution and Examples
- Call to action

# Introduction to Ben Davies And Movìri

- I am Ben, and I am a capacity planner  (Hi Ben)
- I used these tools and techniques as a IT security / audit guy, process improvement guy, and capacity guy over the last 20 or so years.

- Movìri is a global IT consultancy with multiple offices in the US and around the globe
- More than 150 engineers world wide
- Developers of Caplan,  Later to become BMC Capacity Optimization
- Movìri has several lines of business  Testing & Optimization, Monitoring. Operations and Cloud, Security, Analytics, and Capacity Management
- We can help you do this

Our job is **NOT** to
collect, analyze and interpret.

Our job is to **take action**, and we
collect, analyze and interpret
to determine what action is required.

Action is based on compliance to a policy or standard

If you don’t have a
policy or standard to reference,
you should not be looking at the metric.

Windows storage looking for C:\
Min < 51% (underused)
OR
Max > 95% (overused)

Application Response Time
Transactions Per Second

What action?  Who's authority?

What about high CPU?

Primary Goal:
Enforces Policy and Standards
demonstrates someone is enforcing policy

Secondary Goal:
Puts IT issues in business language
Provides the authority to ‘fix it’

# Diversion into Business Risk

What does the business do with a business risk?

Options are:

- Do nothing and take the (increased) risk of being out of compliance
- Change the standard, based on an understanding of the risks for the new standard.
- Become compliant to the existing standard.

Risk strategies - Avoid, transfer, mitigate (monitor, control, contain, prevent), accept.

Action based on compliance to
policy,  standard, business requirement

Why?

To adopt the **authority** of the
policy, standard, or business requirement.

# Find or Make the Policy or Standard

# CIO Policy 12345  Dated 20170101

The Office of the CIO, under authority granted by the Board of Directors prescribes the following Information Systems Standards:

1.001 Response time for **Production interactive applications** will maintain an average sub 2,000 millisecond (2 second) response time for login and basic function as measured from just inside internet connections.  95% of measured response times shall be less than 3250 milliseconds as measured from various continental US testing points using common customer internet connections.

1.002 Response time for **internal interactive applications** will maintain a sub 2500 millisecond response time for login and basic functions, on the corporate network and no more than 3500 millisecond response time for login and basic functions.

…

25.001 Information Technology directors will **develop and maintain standards** for approved Operating systems, programs, utilities, scripts etc., such as approved versions, configurations, use cases, user groups and utilizations of resources.

# An example of a Standard

Under authority granted by of the Office of the CIO, the Director of Servers hereby establishes baseline standards for computer systems.

**33.001 Storage mount point utilization**

.001 \ root directory shall be a separate mount point and shall be protected from becoming 95% fill

.002 \usr and other user type mount points shall not be separated as their own mount point. These directories can be monitored for size, which must be minimal. Servers shall not be used for user activity.

.003 \usr and other user type mounts on devices that are intended to include a number of users shall have a separate directory and space but shall maintain 50% utilization or greater

.004 \core and other core dump directors shall be 75% or greater (not to exceed 200%) of installed physical RAM. These directories shall be monitored for use and kept clear. Core dumps should be set aside or deleted to allow for further core dumps.

.100 Windows C:\ mount points shall be greater than 50% used and less than 90% used. This space should be stable as other mount points should be used for volatile disk writes

# Now for a Compliance Investigation

Pick a standard to monitor / investigate.

The ‘production application 2000 millisecond standard’ for logins let’s say.  There is an expectation that there is instrumentation to directly monitor the response time as described in the standard.

When you find that there is a violation, you should investigate where the bulk of the delay is such that you can make a recommendation.

The resulting note to the application manager could look like this…

# Compliance Note/ Nasty Gram/ Do Better Letter

Mr. or Ms. Application Manager,

**Subject:** Appxxxx policy variation

Performance ticket #3-1415 has been opened on your behalf to address this observation.

A routine review of your application shows that login and basic function does not deliver response times in line with CIO Policy 12345 § 1.001  Dated 20170101

Our preliminary investigation suggested that the link from backend server AppXXX78 to DB901 incurred the most delay.  Your prompt attention is appreciated.

We are here to help in any way we can.

VR.

Splunk  index=responseLog  appxxx responseTime| where responseTime>2000

# And if no Violations??

Monitoring Manager,

Performance ticket #31416 has been opened and closed documenting this review.  No action is needed on your part.

A routine review for compliance with CIO Policy 12345 § 1.001.  Dated 20170101 Public application response time, was conducted today.

**No material noncompliance conditions were observed, for the period under review.**

VR.

Splunk  index=responseLog  appxxx responseTime | where responseTime>2000

I maintained this with
Paper Scrips

# A word about exception conditions

Normal
Normal Exception
Exceptional Exception

This is a very helpful concept not just in this context

# Call To Action

Find or make policy / standards

Audit against the policy / standard

Take action – using the authority of the policy / standard

Run with paper script until ‘well controlled’ then automate

St Louis CMG Meeting

July 17, 2018

# Actionable Intelligence Demands ACTION to Address Business Risk

*Presented to you by:*

*BEN DAVIES*

We make heavy use of the comments section.
Download the presentation for that data.

- **QUESTIONS & ANSWERS**

*Can't think about anything now? Send an email!*

*ben.davies@moviri.com*