The State of System Controls

An Audit Perspective

New York and Tampa Bay RACF User Group

20 April 2016

David Hayes

Compliance is Getting Significant Attention

- A large amount of time and energy spent on controls is now dedicated to achieving compliance with a series of mandates from various sources
- Significant effort is expended mapping large lists of “standards” to how those standards *could* be addressed in various technologies – usually not by specialists knowledgeable of System z
- A preponderance of current “audit” attention is almost entirely based on verifying compliance
- Organizations are dedicating a considerable amount of resources to creating and justifying exceptions to comply with standards being imposed by others.

Are *compliant* systems well controlled?

Compliance = Achieving Control Objectives?

- Without question, any organization *should* be in compliance with all relevant requirements and standards (i.e. compliance defined as a control objective)

- Given the burden of achieving compliance, combined with the constrained availability of qualified resources to work with System z controls, to what degree are the control objectives of organizations driven by complying with standards and regulations created by outsiders (who perhaps may not be cognizant of System z considerations)?

- Does a gap analysis exist of the state of controls achievable by compliance vs. the state of controls that are consistent with the organization's control objectives (defined by mission and corporate values)?

Is Complying with Policy/Standards Achieving a Desired State of Controls?

Examples of recent observations from independent audits:

Controls over APF library access and monitoring

- Full and verified compliance with change control policies and procedures existed
- Access and control monitoring was in place
- Excessive access to APF libraries and lack of logging was identified

Access assignments to prevent incompatible functions assigned to individuals

- All access was assigned consistently with policy (in this case, via automated “provisioning” processes)
- All access assignments were periodically verified for accuracy
- Access assignments creating incompatible functions for individuals existed

Can Being Complaint Blind Decision Makers?

- What are the qualifications of the senior level decision makers who are required to make bottom line decisions, often in the form of certifying compliance with standards and regulations?
- What and who are these senior level decision makers relying on to draw conclusions involving how aspects of System z are controlled and operating?
- Once compliance is declared (victory), does the focus of attention on that specific body of controls fade until the next time the formal declarations of compliance are due?

Compliance Must be Achieved – Effective Controls May be Achieved

Suggestions and thoughts…

- Do the best you can to openly communicate how much of your operation's capacity is consumed with compliance activities
- Bias your activities and communication towards what you know to be proper and correct. Make sure you have solid, factual ground on which to stand.
- Take a hard look at your own policies and procedures – especially when problems are found
- Engage everyone you can and communicate. Know that few are fully satisfied with the current compliance-driven approach to operations, planning and management.