TARGETING AUDIT ATTENTION – STRATEGIES FOR ASSESSING RISK

LEARNING FROM EXPERIENCE

Stu Henderson & David Hayes

New York & Tampa RACF User Group – Nov. 25, 2014

Disclaimer

David Hayes is honored to participate in the RACF User Group. He works with information system controls in support of the U.S. Government Accountability Office's financial audits. The information and opinions presented today do not represent any official positions or views of the Government Accountability Office.

Agenda

- Identify how risk is recognized and managed in the entity
- Identify how risk management activities in the information system business function fits into the entity's risk management process
- Understand how existing audits (internal and external) and assessments address risk
- Develop strategies to target audit attention consistent with risk

Overview

We've seen a lot of audits and a lot of audit surprises. We've found that the starting point (identifying risk) has special characteristics when mainframes are part of the enterprise architecture. As we describe these characteristics to you, you may want to note their affect on audits you conduct or are subject to.

Risk Management at the Entity Level

- Audit attention should be based on a solid understanding of how the entity recognizes and manages risk.
- How does the entity measure risk?
- What are the entity's control objectives?
- How are those control objectives communicated to the information systems business units?
- How does the entity measure achieving control objectives?

Risk Management at the Information System Business Unit Level

- Are information system (IS) risk management processes consistent with the entity's risk management processes?
- How have IS assets been identified and valued?
- How have threats to IS been identified and quantified?
- Have IS control objectives been established (and effectively communicated to staff)?
- How is the effectiveness of IS controls measured?

Coverage of Existing Audits/Assessments

- Does the IS organization map the scope of existing audits and assessments to their inventory of assets and threats?
- How does the IS organization remediate identified control weaknesses?
- To what extent are current control activities – (i.e. monitoring, access reviews) performed primarily to achieve compliance with audits?

Strategies for Assessing Risk

How does the IS organization approach the three types of threats:

- Known Knowns – such as access to system libraries or assignment of powerful access privileges
- Known Unknowns – such as authentication controls for sessions from other "trusted" platforms, access to datasets on DASD shared with other systems without common RACFs, or controls to DB2 objects when both external and internal controls are active
- Unknown Unknowns – such as the introduction of new connectivity resulting from end-user actions, software flaws, or mistakes or malicious actions by users with powerful access privileges

Assessing Risk: Known Knowns

- Threats that are recognized and controls that are defined and managed by the platform owners should be covered by existing internal and/or external compliance reviews – i.e., be part of the entity's system of internal control
- An inventory of these threats and the assets they could affect should be maintained and should drive control activities

Assessing Risk: Known Unknowns

- Threats that are recognized but controls that are not defined or managed by the platform owners should be covered by existing internal and/or external compliance reviews – i.e., be part of the entity's system of internal control
- Special attention should be applied to effective balance between detective and preventive controls
- An inventory of these types of threats and the types of assets they could affect should be maintained and should drive control activities

Assessing Risk: Unknown Unknowns

- The potential for threats is recognized but the exact nature of them is not; however, controls are available to mitigate risk and the implementation of those controls should be part of the entity's system of internal control
- Special attention should be applied to effective risk mitigation strategies
- Periodic risk evaluations and regular risk identification activity (such as industry research) should be on-going

(General) Risk Based Audit Strategies

- Evaluate the effectiveness of the criteria used for routine compliance activities
- Evaluate if valuable assets really are accurately and completely identified and inventoried and used to drive control activities
- Determine if a healthy level of segregation of duties/influence really exists between system operations, access control, change control, storage management and monitoring control functions

(General) Risk Based Audit Strategies

- Measure the entity's responsiveness to control information that should trigger follow-up action
- Identify exactly what risk management information is provided to decision makers and how often (is it just the red/yellow/green indicators in some nifty Windows pop-up?)

(Specialized) Risk Based Audit Strategies

- If any DB2 systems are in transition between internal and external control, look closely at the control strategy in place during and at the completion of the transition
- Identify who owns and manages controls over all the different access paths into the mainframe. Are the end-points of those controls known and centrally managed/supervised by individuals with appropriate skills and authority to effectively manage risk?

(Specialized) Risk Based Audit Strategies

- Are storage functions/controls being relied on as access controls? If so, audit them using the criteria applicable to access controls.
- Is the entity effectively using the analytic capabilities of their systems and software products to recognize threats and manage risk?

Summary

- Identifying Known Known Risk, Known Unknown Risk, and Unknown Unknown Risk should be embedded in any entity's risk management approach
- On-going evaluation and assessment of risk must be on-going/staffed/recognized parts of routine business if risk management is to be effective
- Audit surprises mean that something isn't happening or isn't happening at the right times

Contact Information

- Stu Henderson stu@stuhenderson.com
  www.stuhenderson.com (301) 229-7187

- David Hayes hayesd@gao.gov
  www.gao.gov (202) 512-6306