How Internal Control Translates into RACF

New York and Tampa Bay RACF User Group

David Hayes – U.S. Government Accountability Office

15 March 2017

Speaker Introduction

David Hayes is an information systems auditor with the US Government Accountability Office. His work primarily supports assessments of internal control over financial reporting in the context of information systems.

The opinions expressed in this presentation are David's and do not necessarily reflect the views of the US Government Accountability Office.

Internal Control – A Process

Five Elements of Internal Control:

Do

1. Control Environment – the organization's values and goals set and demonstrated by the senior leaders
2. Communication – dissemination of the organization's goals, control objectives and policies
3. Assessing and Managing Risk – identify assets and threats and establishing quantified risk management policies
4. Control Activities – probably much of what you do at work
5. Monitoring – measuring how #4 is satisfying #2

Loop until OutofBusiness() or Retirement(!)

Controls – Focus On Financial Reporting

Controls over financial reporting will involve your organization’s assertions over the following:

- Accuracy – recorded transactions are reflected correctly in financial statements
- Prevention and Detection of Errors (including fraud) – initial data entry and subsequent processing/reporting
- Existence – recorded transactions happened and relate to the entity
- Completeness – all transactions are included in financial reporting

Accuracy Controls Over Financial Reporting in Systems

- Financial application components are strongly protected from out-of-process changes – supporting management's assertion that processing is repeatable (this enables the auditors to test samples of transactions)
- Controls clearly divide access between financial data that are used for reconciliations whenever possible
- Any type of privileged access (application or system level) is tightly controlled

Prevention and Detection of Errors

- Master data and transaction data are clearly labeled and subject to different levels of access and detection controls
- Access controls are carefully designed and implemented to divide incompatible duties (application and administrative level)
- Granular detective controls are actively implemented – patterns of potentially anomalous activity are detectable
- System owners actively create processes involving dual controls to prevent an individual from creating errors

Existence Controls

- Business logic creates process flows that force multiple individuals to create purchase/financial transaction requests, approve those requests, process the acceptance of the good/service delivered and make the resulting accounting entry
- RACF must be configured to robustly support keeping access to process flows divided between individuals (segregation of incompatible functions and dual controls)

Completeness Controls

- Providing a level of certainty that all financial transactions are included in financial reporting is one of the most difficult accounting assertions to support
- Any level of data access that creates the potential for alteration of data outside of the normal business processes must be tightly controlled
- Logging that allows for positive assurance that out-of-process access to data DID NOT occur over specific time periods is very valuable

Conclusions

RACF can effectively support specific business control requirements when:

1. Exact control requirements are known
2. Application and system architectures are compatible with internal control requirements
3. Tools are implemented to support effective use of logs
4. Effective naming conventions are used
5. RACF controls are clearly labeled and documented (internally and externally)
6. Business owners are actively involved in the operations of controls