MacEwan UNIVERSITY | OFFICE OF THE CHIEF INFORMATION OFFICER

Segregation of Duties

Standard D8010-3

Effective Date: April 27, 2017

Authority & Alignment

Authority: Employee Code of Conduct; D3300 Internal Controls; D8010 Information Security and Identity Management

Alignment:
International standards – Cobit, ACFE Fraud Classification System, ANSI INCITS 359-2004 RBAC Reference Model

Overview

The purpose of segregating responsibilities is to prevent occupational fraud and errors. A fundamental element of internal control is the segregation of certain key duties. The basic idea underlying Segregation of Duties (SoD) is that no employee or group of employees should be in a position both to perpetrate and to conceal errors or fraud in the normal course of their duties.

The general premise of SoD is that an individual should not be able to initiate, approve, and review the same action. The flow of transaction processing and related activities should be designed so that the work of one individual is either independent of, or serves to check on, the work of another.

SoD is often correlated with logical system access. While not incorrect, this approach may overlook the importance of understanding business risks and existing and/or compensating controls already in place to address those risks.[1]

Scope and Definitions

This standard applies to all business processes and applications at MacEwan University (the "University"). It also applies to administrative and privileged system access.

System Owner: Synonymous with Data Owner. A person who is responsible for the overall development, integration, modification, or operation and maintenance of the information system and is used in relationship to change control, system and data access, Service Level Agreements, and a sustainment and security partnership with the information technology service provider. More specifically, System Owners:

1. Establish and communicate service level requirements with IT.
2. Define the functions, procedures, reports and audit requirements of the system.
3. Ensure an adequate training plan is prepared and delivered to the system users.
4. Ensure the design, development and testing of the system leads to appropriate functional standards.
5. Working with IT, authorize system changes. (outages, changes, emergency changes, etc.)
6. Working with IT, manage and authorize access to data.

[1] The text of this Overview is taken largely from an article by Nick Stone in the April 2009 issue of Internal Auditor Magazine entitled "Simplifying Segregation of Duties".

7. Working with IT, maintain and review data security and integrity.
8. Define, approve and manage user access and permissions.
9. Participate in governance and planning activities to inform enterprise architecture.

Compliance & Exceptions

Responsibility for compliance with University policies and standards extends to all members of the University community. Non-compliance may create risk for the University and will be addressed accordingly.

Standard Requirements

1. The University's System Owners are responsible for defining, justifying and maintaining adequate Segregation of Duties (SoD) for their business processes.
2. System Owners will maintain a matrix, or other listing, of incompatible job functions.
3. IT will maintain a matrix, or other listing, of administrative and privileged system access.
4. The IT Compliance function will conduct an annual review of administrative and privileged access for IT Staff to ensure adequate SoD.
5. System Owners will use a risk management process to:
    a. Identify the critical risks in role design and assignment that have the potential to result in fraud or error.
    b. Map risks to SoD conflicts for key business processes.
    c. Prioritize conflicts by considering variables that impact the likelihood and magnitude of potential fraud or error. Variables can include the nature of financial transactions, the nature of vulnerable assets, exposure to identity-related fraud, the effectiveness of role-based access controls, and the degree of compensating controls that could prevent or detect fraud or error. Compensating controls can be manual, system-based, or organizational in nature.
    d. Review all shared accounts accessible by non-IT staff and develop appropriate compensating controls based on risk assessments.
    e. Document risk assessments clearly, describing all risks that are evaluated. Provide the rationale used to identify, prioritize, and disposition risks.
6. If risk response requires modifications to existing roles, those modifications will be implemented through a process that documents the request, review, approval and implementation of the modification.

Related Content

Type	***Title***
Policy	D7110 Fraud and Irregularities
Standard	D8010-2 Role Design Standard
Standard	D8010-1 Information Security Framework Standard

Measurement

- ✓ Documented risk assessment
- ✓ Matrix, or other listing, of incompatible job functions
- ✓ Documentation of role modification including approved Change Requests

Contact

Director, IT Compliance and Information Security Office