
AUDITCON
A HIGHER EDUCATION SUMMIT
ACUA
ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

Performing a Privileged Access Management Audit

AuditCon
A Higher Education Summit
September 24-28, 2023 Loews Miami Beach Hotel • Miami Beach, FL

Speakers

Edie Chung, CPA, CISA
Principal Auditor
Office of Audit, Risk and Compliance
Duke University

Jocelyn Edge, CPA
Principal Auditor
Office of Audit, Risk and Compliance
Duke University

Mark Ledman, CPA, CISA
IT Audit Manager
Office of Audit, Risk and Compliance
Duke University

Session Objectives

Identify Privileged Roles

Participants should be able to identify privileged roles and user accounts based on permissions and job responsibilities at the application level.

Assess Risk Factors

Participants will assess HigherEd risk factors including sensitivity of data, regulatory compliance, and proprietary information to select appropriate applications for testing.

Plan & Perform the Audit

Participants will have the knowledge to plan and perform an independent, objective PAM audit for any application.

What is Privileged Access Management?

What is Privileged Access Management?

Privileged Access

Privileged access gives the user a higher level of access to resources and infrastructures than would be granted to the user of a standard account.

Privileged Access Management

Privileged Access Management (PAM) is the combination of tools and technology used to secure, control and monitor access to an organization's critical information and resources.

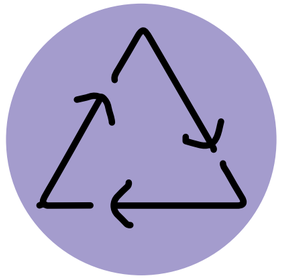
Privileged Access Management

WHAT IT
IS & IS NOT

Effective Method to Assess Logical Access Controls

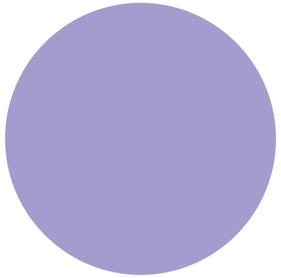
Privileged Identity Management (PIM)

An Opportunity to Strengthen Application Security



Full Logical Access Audit

Education Opportunity for Stakeholders



Identifying Privileged Access

DOMAIN ADMIN

EMERGENCY ACCOUNTS

DEVELOPER

DATABASE ADMIN

SUPER-USER

SYSTEM ADMIN

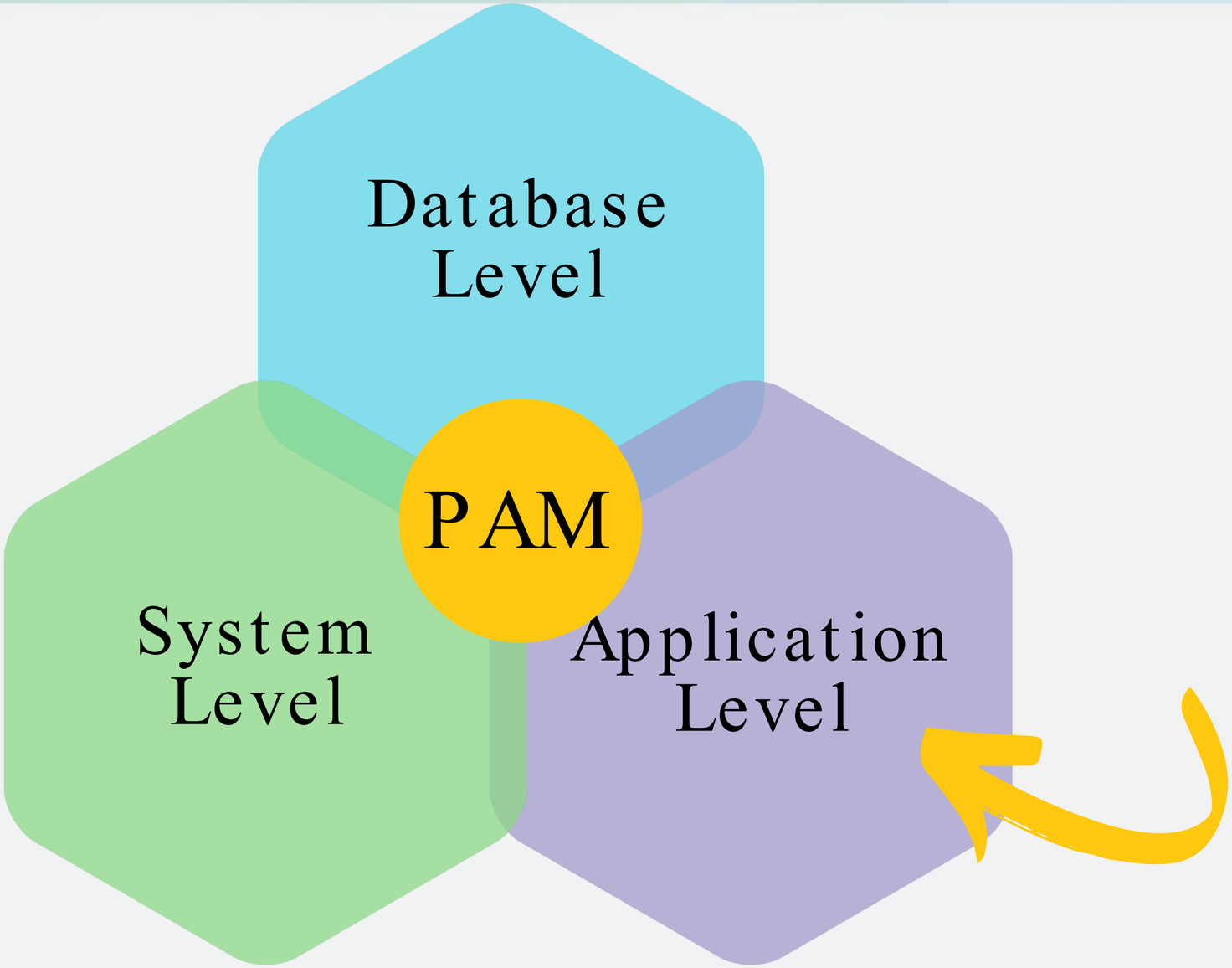
PARENT/ OWNER

BREAKGLASS

ROOT ACCOUNT

SERVICE ACCOUNT

Types of PAM Audits



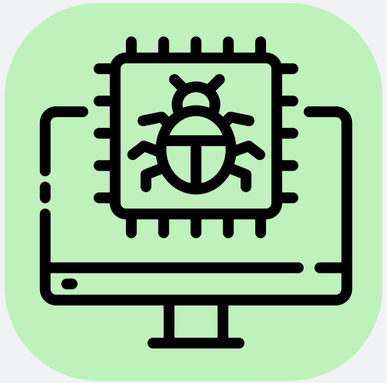
Key Risks & Controls

ACUA
ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

Significant Risks and Security Vulnerabilities

Data Breach

Insider Threats

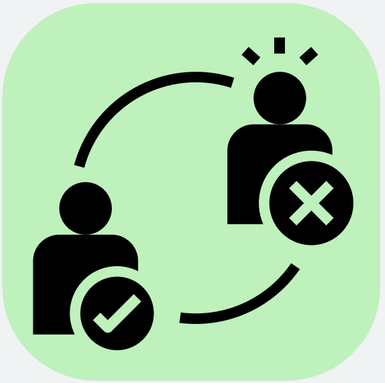


Malware & Ransomware

Unauthorized System Changes

Compliance & Regulatory Violations

Privilege Escalation Attacks



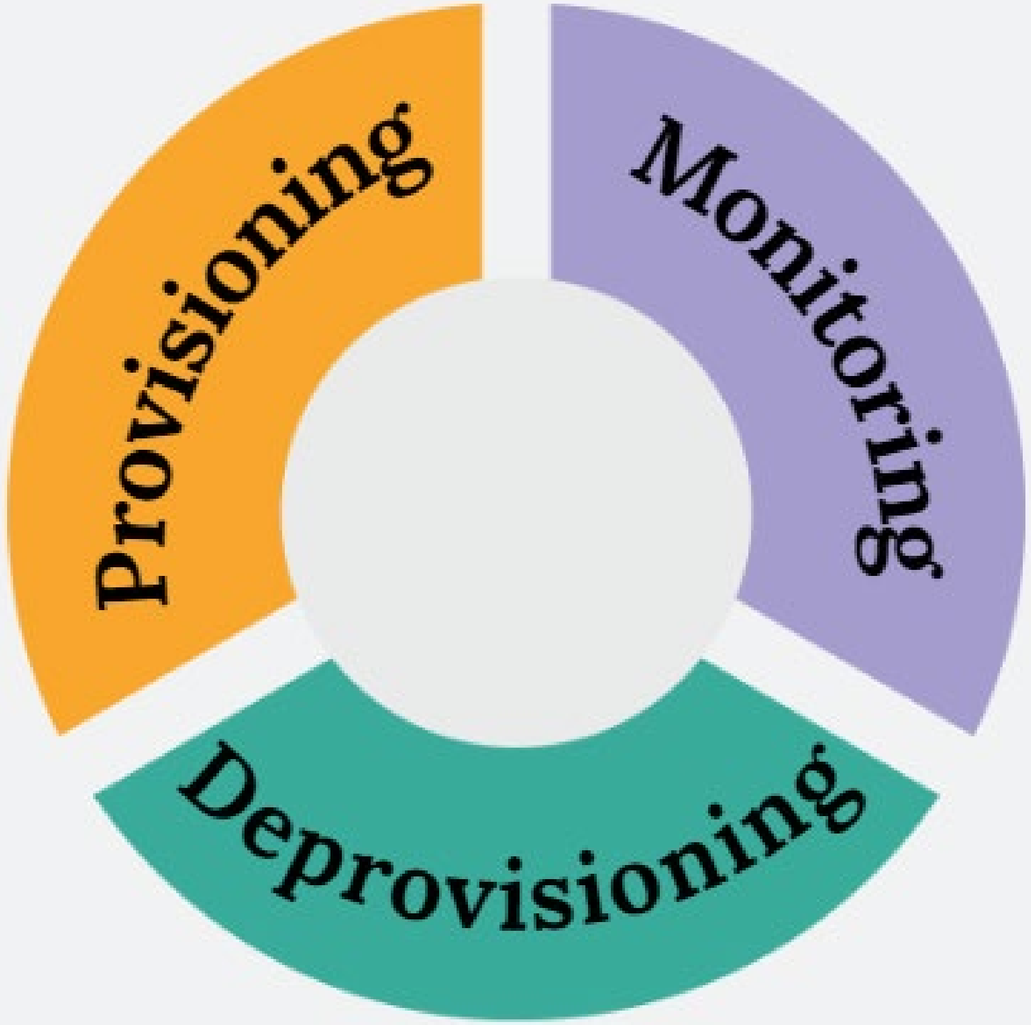
User Impersonation

Unauthorized Service & Application Access

Human Error

Disrupt Critical Business Operations

Key PAM Controls



Provision Controls

- Authentication: Verifying the identify of users or entities requesting or granting access
- Authorization: Authorization of the appropriate level of access from applicable level of management
- Role-Based Access Control (RBAC): Automated assignment of permissions and access based on an individual's role within an organization.
- Least Privilege Principle: Granting the least amount of privileges possible for an individual to perform their job function
- Approval Workflow: Request and approvals through a formal process

Deprovision Controls

- Employee Offboarding Process: Integrate access deprovisioning into employee offboarding processes, so when an employee's status changes, this integration will trigger automated deprovisioning.
- Role-Based Deprovisioning: If you have RBAC, deprovisioning can be aligned with this system to ensure as roles changes, access rights are adjusted or revoked based on the role (this captures transfers).
- Periodic Access Reviews: Conduct regular access reviews to identify dormant, unused or inappropriate access.
- Training & Awareness: Train employees, managers, and IT pesonnel on the importance of timely access deprovisioning.

Monitoring Controls

- Real-Time Monitoring: Capture and analyze privileged user activities as they occur to immediately detect unusual or unauthorized activity.
- Alert & Notifications: Enable alerts and notifications when predefined events or anomalies occur to allow prompt responses to security incidents.
- Logging/ Audit Trails: Maintain comprehensive logs of privileged user activity, including failed log in attempts, changes to system configurations and access to sensitive data.
- Periodic Reviews: Conduct regular reviews of logs to identify unusual, suspicious, or inappropriate activity.

Planning a Privileged Access Management Audit

Overview of PAM Audit*

PLANNING

Ensure scoping high-risk applications and applications with sensitive data; Consider client input.

FIELDWORK

Consider factors that may influence sampling methodologies

WRAP-UP

Use findings as "opportunities for improvement" and educate clients to empower them.

Planning

HIGH RISK OR CRITICAL BUSINESS APPLICATIONS

APPLICATIONS CONTAINING STUDENT, HEALTH SYSTEM OR OTHER SENSITIVE DATA

APPLICATIONS DEEMED IMPORTANT BY THE CLIENT

Fieldwork

Factors Influencing Sampling Methodology

Sensitive Data

The type and sensitivity of data contained in an application may influence the applications risk profile

Institutional Value

Enterprise usage or executive leadership opinion may influence the perceived risk profile of an application

Number of Users

A high volume of privileged users can require a larger sample size and increased scrutiny of relevant business case

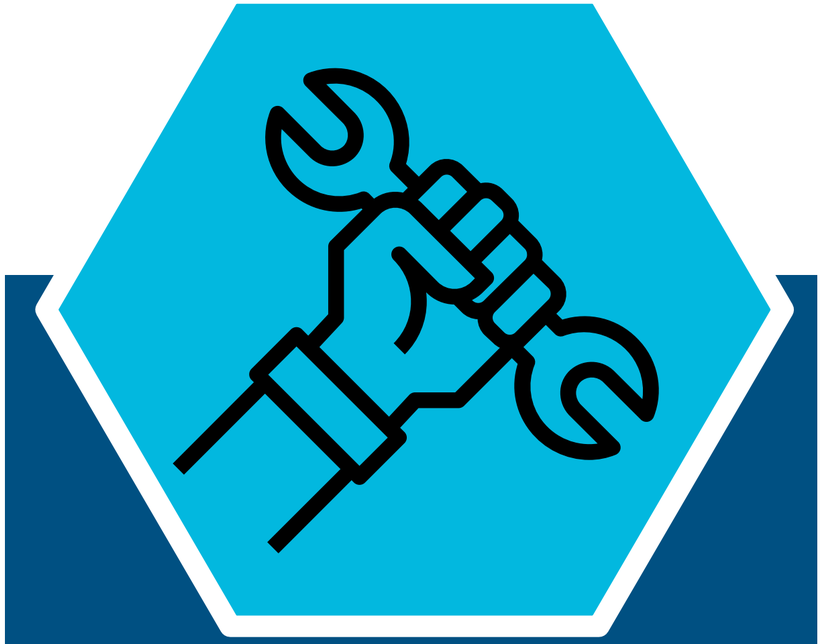
Sign on Methodology

Single sign on and multi-factor authentication and biometrics can reduce risk and thus reduce sample size

Application Development

Internally developed vs. externally developed; web facing vs. firewall protected are relevant considerations

Wrap Up



REMEDY

EDUCATE

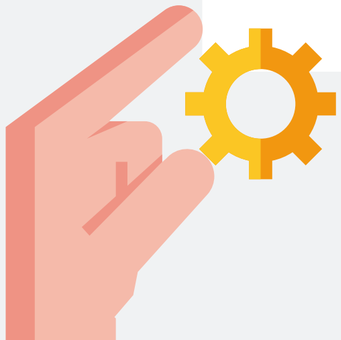
COMMUNICATE

Common Audit Findings

ACUA
ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

Common Audit Findings

- Lack of provisioning/ deprovisioning controls
- Lack of enabled logging or logging capabilities
- Lack of monitoring controls
- Terminated/ transferred accounts still active
- Shared privileged account



Interactive Session

Answer to Scenario(s)

Answer to Scenario(s)

Answer to Scenario(s)

Tips & Tricks

ACUA
ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

Tips & Tricks to an Effective PAM Audit

Utilize a Questionnaire

Practice "Least Privilege" Principle

Try a 'Just In Time' Model

Obtain an application inventory

Leverage any PY Audit Work

Thank You!

Edie Chung
Edie.Chung@duke.edu

Mark Ledman
Mark.Ledman@duke.edu

Jocelyn Edge
Jocelyn.Edge@duke.edu

Want to learn more about Privileged Access Management?

View ACUA's PAM Kickstarter!

https://acua.org/Audit-Tools/ACUA-Kick-Starters