Identity & Access Management in an Academic Environment

Webinar
May 17, 2018

Johan Lidros CISA, CISM, CGEIT, CRISC, HITRUST CCSFP, ITIL-F
President Eminere Group

ACUA

ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

Did you know that Connect ACUA allows you to post new messages directly from your email without logging in to the Connect ACUA website?

For more details, check out the Quick Tip post on

Connect.ACUA.org

Your Higher Education Auditing Connection

ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

Use a Kick Starter to launch your next audit!

ACUA Kick Starters

- Developed by ACUA members (Subject Matter Experts)
- Higher Education Specific Topics

www.ACUA.org → Resources → Audit Tools → ACUA Kick Starters

Do you have a great idea for an ACUA Kick Starter?
Contact Justin Noble at Justin.Noble@ttu.edu

Association of College and University Auditors

ACUA

ASK NOT WHAT YOU CAN DO FOR ACUA BUT WHAT ACUA CAN DO FOR YOU!

Stay up to Date

News relevant to Higher Ed internal audit is posted on the front page. Articles are also archived for your reference under the Resources/ACUA News.

The College and University Auditor is ACUA's official journal. Current and past issues are posted on the ACUA website.

WWW.ACUA.ORG

ACUA SOCIAL NETWORKING

Connect with Colleagues

- Subscribe to one or more Forums on the Connect ACUA to obtain feedback and share your insights on topics of concern to higher education internal auditors.
- Search the Membership Directory to connect with your peers.
- Share, Like, Tweet & Connect on social media.

Get Educated

- Take advantage of the several FREE webinars held throughout the year.
- Attend one of our upcoming conferences:
- Midyear - March 18-21, 2018 Hyatt Regency Hotel, Louisville, KY
- Annual - September 9-13, 2018 New Orleans Marriott, New Orleans, LA
- Contact ACUA Faculty for training needs.

Get Involved

- The latest Volunteer openings are posted on the front page of the website.
- Visit the listing of Committee Chairs to learn about the various areas where you might participate.
- Nominate one of your colleagues for an ACUA annual award.
- Submit a proposal for the conference.
- Write an article for the C&U Auditor.

Solve Problems

- Discounts and special offers from ACUA's Strategic Partners
- Risk Dictionary
- NCAA Guides
- Resource Library
- Vendor Directory
- Governmental Affairs Updates
- Survey Results
- Career Center.....and much more.

WEBINAR MODERATOR

ASSOCIATION OF COLLEGE & UNIVERSITY AUDITORS

Advancing Auditing in Higher Education

- Don't forget to connect with us on social media!

ACUA SOCIAL NETWORKING

ACUA Distance Learning Director

Amy L. Hughes

Director of Internal Audit
Michigan Technological University

Presenter

- Johan Lidros, Founder and President of Eminere Group
- Has provided information technology governance and information security services in the Higher Education and Healthcare industries for 20 years in Europe and in the United States
- Well-versed in accepted IT and information security standards/frameworks (ISO27000, HITRUST, NIST, COBIT, CIS, etc.) and has participated in several related committees
- Certifications: CISA, CISM, CGEIT, ITIL-F, CRISC, HITRUST CCSFP

Table of Contents

Introduction

- **Session Objectives:**
  - Objective 1: Common “best” practice identity and access management
  - Objective 2: How to audit identity access management to address the root causes
  - Objective 3: Tools and resources for access management best practice
  - Objective 4: Key measurements to drive operational change

Introduction

- **Most IT audits find identity and access management issues related to areas such as:**
  - Number of privileged users (separation of duties)
  - Not approved service accounts
  - Terminated employees
  - Inappropriate access
  - Access to privileged accounts passwords
  - External “workforce” members access
  - No regular review of access in applications, databases and servers (OS).
  - And more…

- **Why can organizations not get this right?**

- **Why do we have repeat findings year after year?**

The Solution – Identity and Access Management

- **Providing the right people with the right access at the right time.**
- **And then over time being able to prove it.**
- **Also, proving that access is changed as peoples roles change and that you have removed access when they leave.**

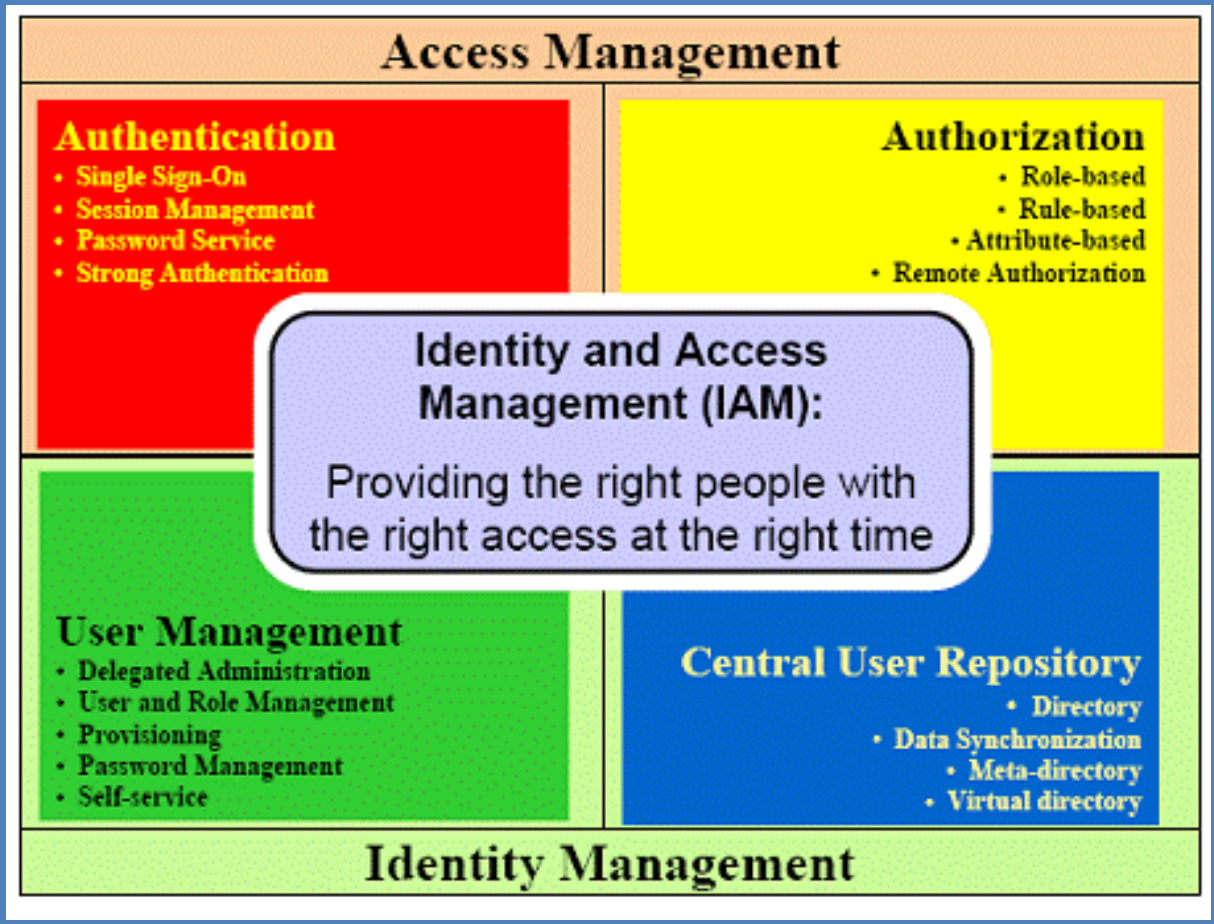
IAM – Strategic Impact

- **How critical is IAM for the organizations success?**
  - Operations
  - Financials
  - Intellectual Property
  - Cyber risk
  - Research
  - Safety
  - Student/Employee/Researchers Satisfaction
  - Recruiting the best (professors, students, etc.)
  - …

What is IAM?

IAM Program

Governance



IT Governance - IT Security Governance – IAM

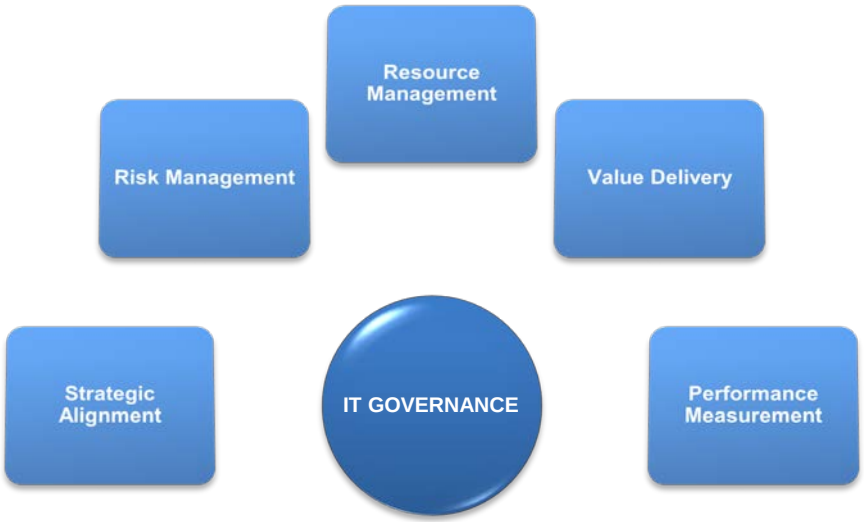


Table of Contents

Typical Environment – Higher Education

- **~200 – 1000 “systems”**
- **How do we define systems?**
  - OS and servers (unix, windows)
  - Databases
  - Applications
  - Mobile Apps
  - Facility systems (badge, power, AC/Heat, cameras, etc.)
  - Network devices
  - Utilities and Tools – job scheduling systems, source code repository, virtualization (Vmware), firewalls, routers, sharepoint, others?
  - Medical Devices
  - Etc.

Typical Environment – Higher Education

- **What do you currently audit?**
  - Application layer
  - Database layer
  - OS layer
  - What systems?
    - Application
    - Utilities – hypervisor, password vaults, badge access, backup scheduler, etc.

Question 1

What is your most critical system?

1. Financial/Student administration system
2. E-learning
3. Facility systems (badge, heat, cooling, power, etc.)
4. Password/encryption key/certificates vault
5. Do not know

Most Common Audit Areas

- Identity and Access Management
- Financial Systems
- Core Business System
- IT General Controls
- HIPAA
- Vendor Management
- Business Continuity and Disaster Recovery
- Network Security
- PCI
- Mobile Device Management
- Patch Management
- Cybersecurity
- New Systems

Additional Key Risks to Audit

- **Health IT**
  - Internet of Things
  - Telehealth
  - Apps (internet of things)
  - Risk Management
  - Medical Devices
- **Data Warehouse**
- **Information Governance**
- **IT Governance**
- **Student/Patient Communication/Portal**
- **Backup Management**
- **Security Awareness Training**
- **GDPR**

Added Value Audits – Hidden Opportunities

- **Life Cycle Management**
  - Application/Tool functionality
  - Tools
  - Cost
  - Age
  - Utilization
  - Budget/capacity/acquisition processes
- **Identity and Access management**
  - Number of systems
  - Authentication
  - Resources for management of access management (FTE/cost)

Audit – Identity & Access Management ?

- **Enterprise risk analysis and risk based audit plan**
  - What is the audit universe
- **Perform risk analysis to determine scope of audit.**
  - Do we really perform a risk analysis or do we just audit what we always audit?
- **Perform the audit**
- **Identify control gaps/issues**
- **Generate recommendations (report, etc.)**
  - What do we typically recommend?

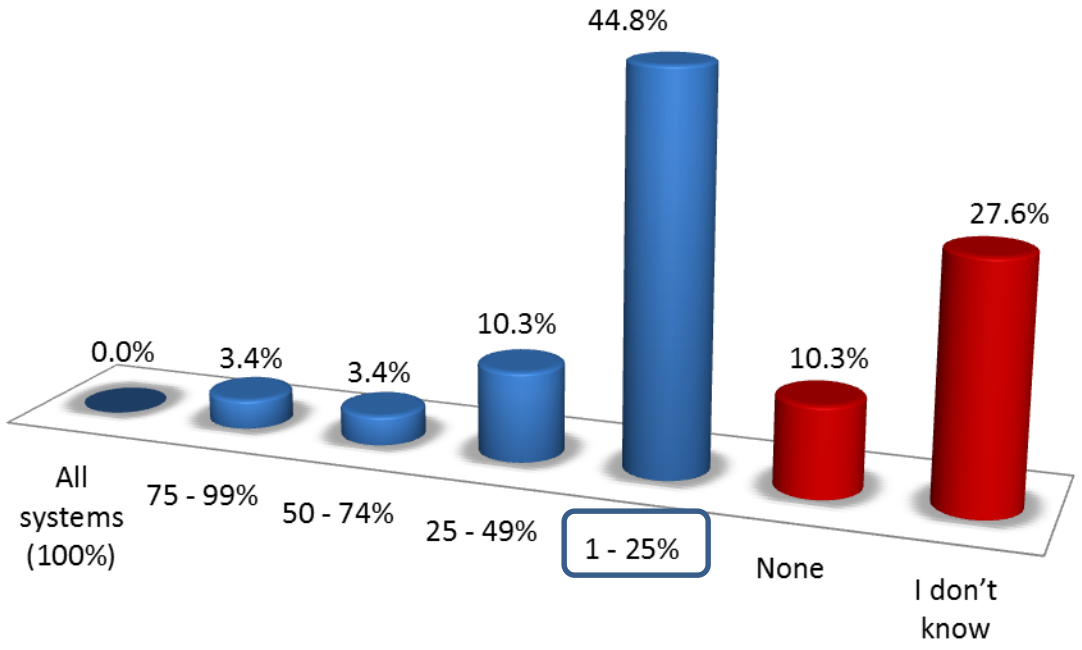
Question 2

If access reviews are performed, for what percentage of your systems are reviews performed?

1. All systems (100%)
2. 50% to 99%
3. 25% to 49%
4. 1% to 25%
5. I don’t know

Scope of Access Reviews

For what percentage of your systems are reviews performed?



Common IAM Audit Findings

- Inappropriate access/ Separation of duties
- Shared accounts
- Lack of approvals
- No regular reviews/confirmation of access and privileges
- Excessive number of administrators/privileged users
- Service accounts
- Duplicate/multiple user IDs
- External “workforce” access….
- Role based access not fully implemented
- No clear business stakeholder/Information owner
- “shadow IT”/decentralized IAM functions

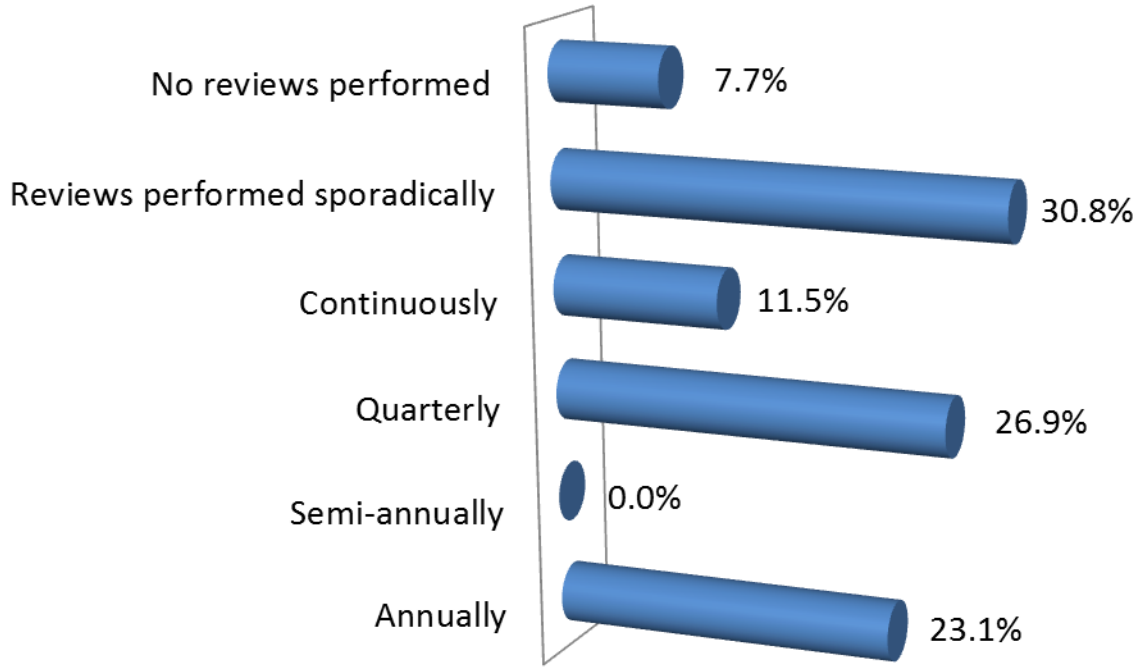
Question 3

How frequently are formal access reviews performed in your organization:

(Access reviews - Validating access to systems based on approval by the system/data/business owner)?

1. Annually
2. Semi-annually
3. Reviews performed sporadically
4. No reviews performed
5. I do not know

Frequency of Access Reviews 2016-2017



No established or implemented policy for frequency of access reviews

Table of Contents

Root Causes

- **Why do we continue to have the same issues re-occurring?**
- **Wrong audits?**
- **Wrong scope?**
- **Wrong recommendations?**
  - Are we just recommending a temporary fix or addressing the root cause?
- **What if we make the right recommendation?**
  - IT or Management not addressing the issue – why?
    - Lack of funding
    - Resources
      - Not enough resources
      - Don't have the right resources
    - Not a 'priority' – how do you balance fixing the issues vs addressing academic/research/administration or clinical related needs?

Root Causes

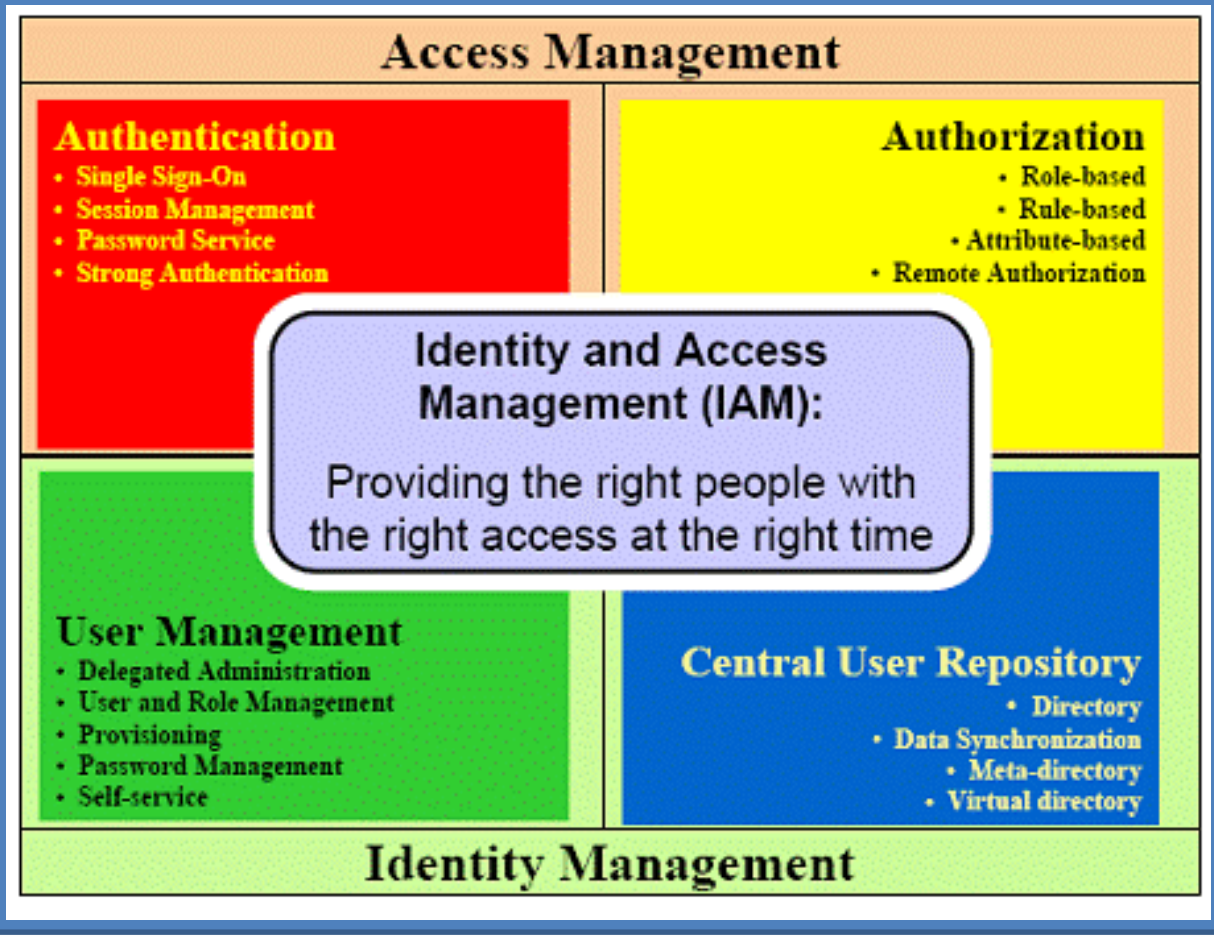
- **No or limited IAM program**
- **Lack of information for decision making**
  - Wrong type of audit
  - Skillset audit team
  - Wrong observation
  - Wrong recommendations
- **Roles and Responsibilities**
  - Accountability (information owner/custodians)
  - Prioritization
  - Ownership of the program
- **Tool Support for IAM**
  - Implementation
  - Wrong tool(s)
- **Resources/prioritization**
- **....**

Table of Contents

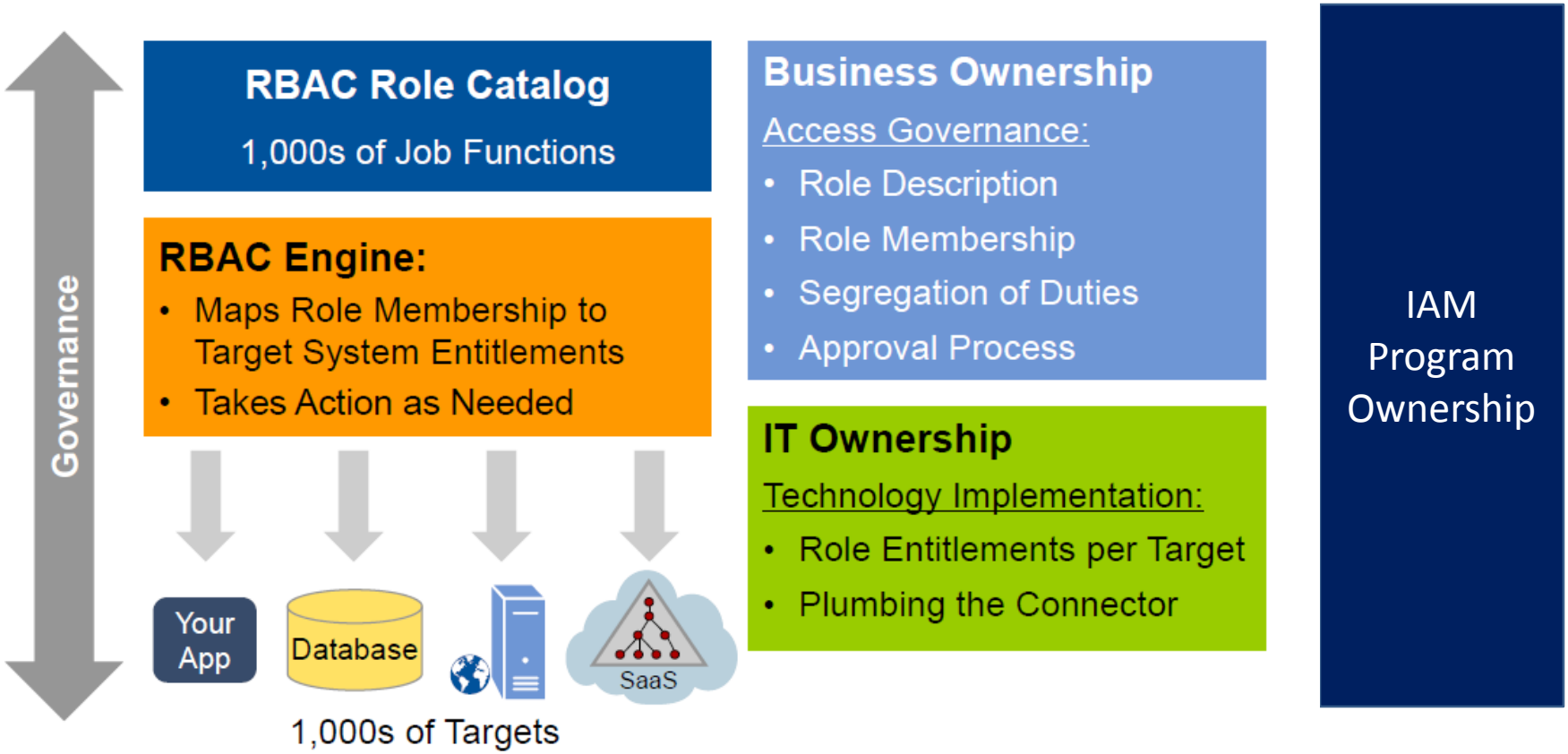
What is IAM?

IAM Program

Governance



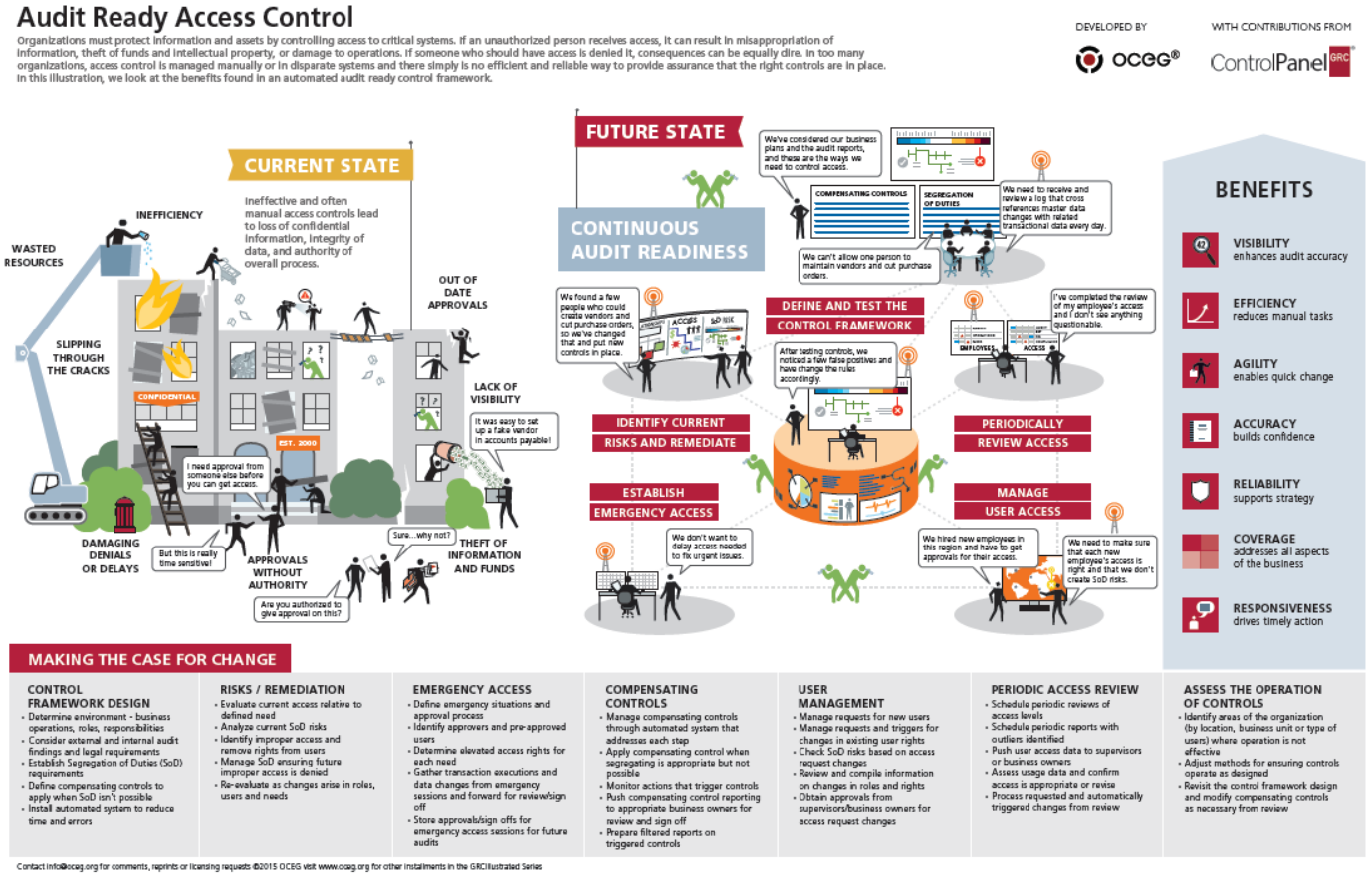
IAM - Implementation



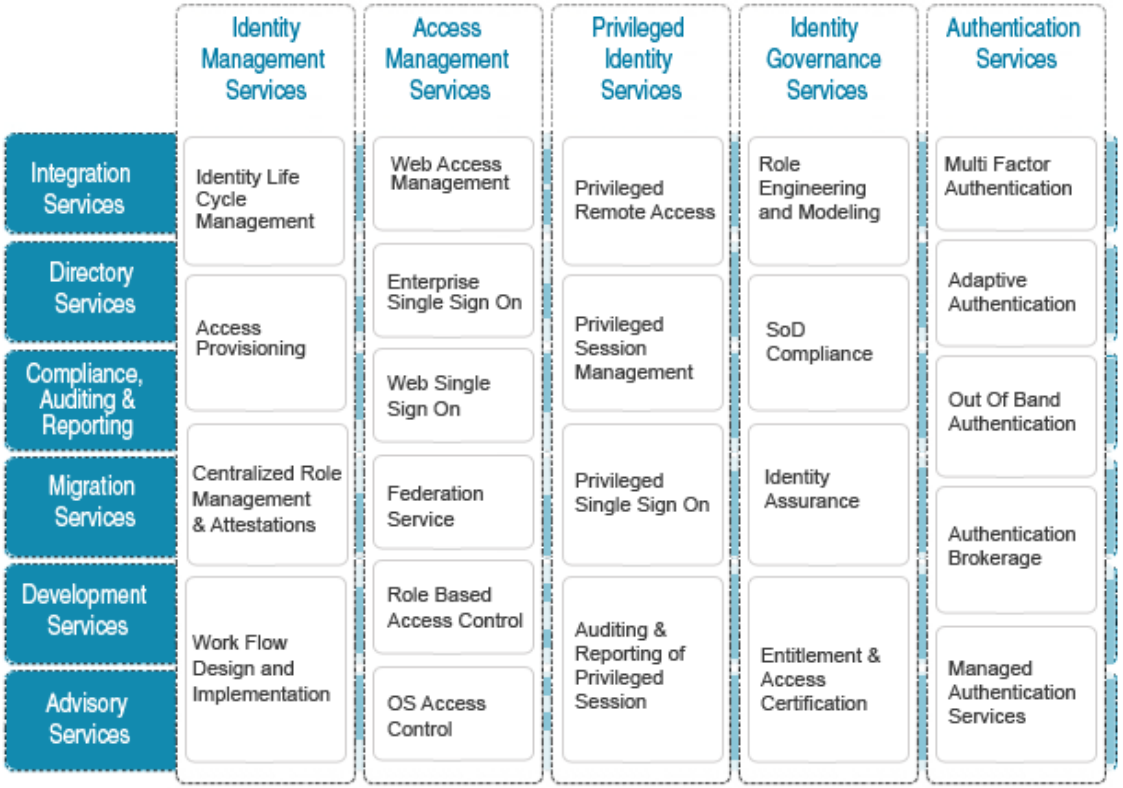
IAM

- Identity Management Services (IAM life cycle)
- Authentication Services (2FA, AD etc.)
- Access Management Services (role based, SSO)
- Privileged Account Management Services
- IAM Governance (SOD, regular reviews, monitoring, metrics, etc.)

Processes – OCEG framework



IAM – Areas and Processes …



Question 4

Have you implemented two-factor authentication as part of your log in process? Please select all that apply.

1. For all users
2. For remote access only
3. For privileged users only
4. Have not implemented two-factor authentication
5. I do not know

Current U.S. Privacy Rules Environment

Laws, regulations, and policies for patient consent

Laws, regulations, and policies for sensitive information

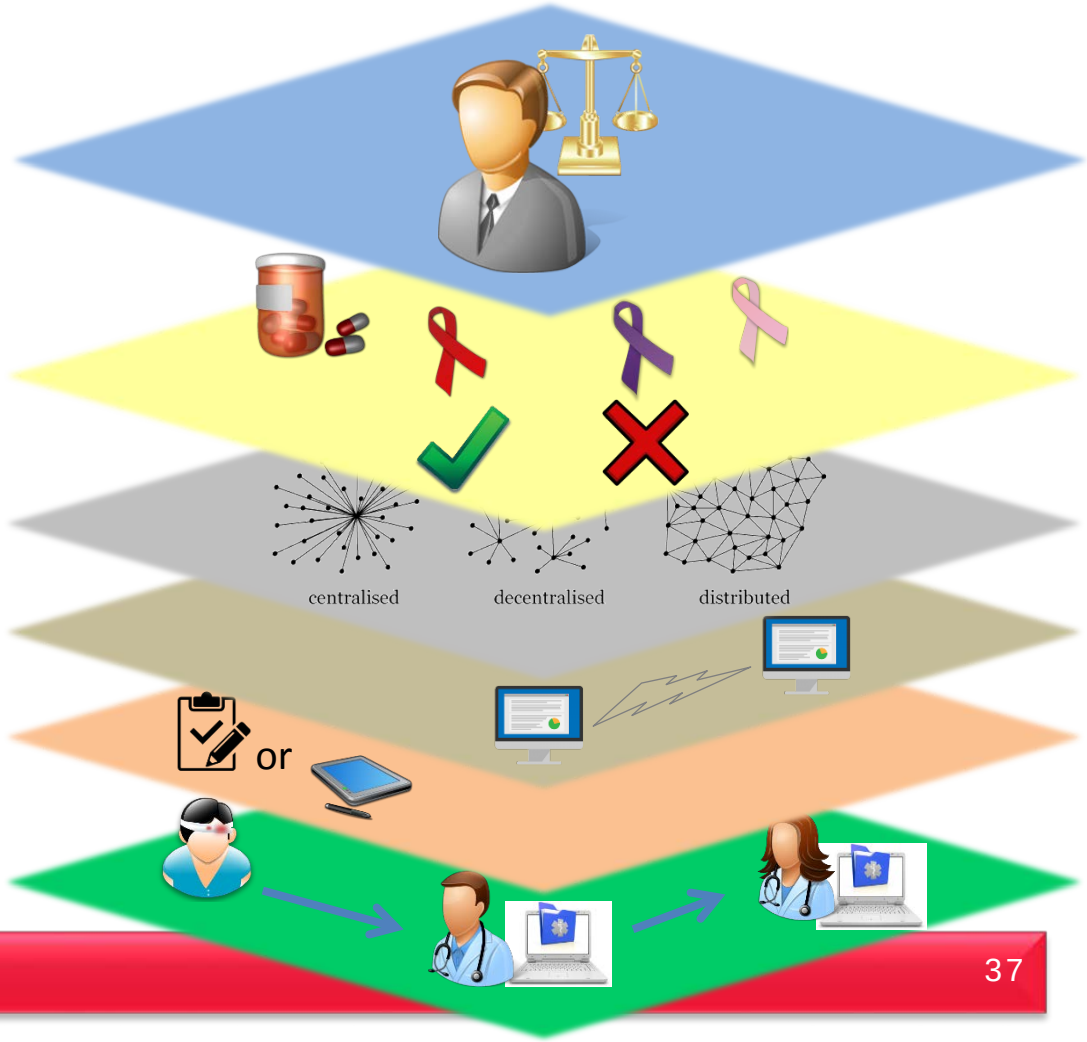
Consent models (opt-in, opt-out, with restrictions, etc.)

Architecture

system interoperability

Consent directive (paper/electronic)

User provides consent to share sensitive information and Permitted Uses and Disclosures



Why IAM Fails

Reason #5: **Failure to plan/govern/fund/prioritize.**

Reason #4: **Failure to engage the proper stakeholders.**

Reason #3: **Automating the existing flawed processes.**

Reason #2: **Trying to "Boil the Ocean" with a "Big Bang" approach.**

And, the #1 Reason IAM projects fail:

Treating IAM as a Stand-alone IT Tool

Success Factors

- ✓ Focus more on process than technology.
- ✓ Implement a sound IAM program that embraces common governance, architecture, and project management.
- ✓ Treat core project team like your family:
  - Long-term continuity, retention incentives.
  - Avoid people churn — causes fits and starts.
  - Insulate team from mindless business distractions.
- ✓ Invest in a strong IAM champion/evangelist:

Sample Key Measurements

- **Number of resources – performing access management related tasks**
- **Number of audit findings**

		Trend	Goal
Type and Number of Systems			
PHI	242	↓	150
PII	312	↑	250
Critical	85	↓	75
Number of FTE IAM	4	←	6
Number of Access Reviews	52 (15%)	↑	80%
Number of Access requests		↑	
-Initial	2300	↑	
-change	500	←	
-Terminations	500	↓	

Sample Key Measurements (cont.)

	Trend	Risk Level
Terminated Users		
Centralized Systems	↑	M
Decentralized Systems	↓	H
Cloud	↑	H
Appropriate Access	←	H

Academic Best Practice – What does it mean?

1. Implementation of a formal Identity and Access Management Program
2. Definition of binding clear Policies for all Stakeholders
3. Business stakeholder/Information Owner/Data Owner
4. Use of Two-Factor Authentication in key areas
5. Privileged Account Management
6. Time limit of access
7. Regular "Certification of Access"
8. Tools
    1. Central IAM solution
    2. Partial central repository of users
    3. Partial central repository of systems

Question 5

Has your organized defined formal metrics related to the effectiveness of the identity and access management program that are reported to management on a regular basis (such as number of systems with formal access reviews, systems in compliance with password policy, etc.)?

1. Yes
2. In the process of being defined and implemented
3. Partial (some schools, type of systems, etc.)
4. No
5. Do not know

Table of Contents

Proposed Audit Approach

- **Full scale audit of Identity Access Management**
  - Not just controls based audit – effective and efficient/value
  - Need to include decentralized, cloud based solutions in addition to centralized solutions
  - Assess resources
  - Assess tools
  - Assess processes
  - Measurements
  - Total cost of ownership
  - Recommendations
    - Need to address root cause
    - Need to be prioritized
    - Need to be risk based
    - Need to assign business stakeholder(s as appropriate
  - Need to perform follow up / status reviews of prior audit findings

IAM - Goals

- Scalable and sustainable system
- Streamlined management of user identities and access rights
- Automate and reduce the time of assessments and reports
- Establish strong privacy and security policies not only within the enterprise but also throughout participation and interaction with external “exchanges”.
- Reduce overall cost of compliance (i.e., audits, penalties, remediation, etc.)

Solution Drivers

- **Business -** lowering the cost of managing employees' permissions and minimizing the amount of time that users are without their necessary permissions;
- **IT Security -** ensuring information security, integrity, and availability;
- **Safety** – Improve risk management
- **Strategic** – ensure business alignment improve key strategic needs/initiatives (business partner initiatives,research, professors/students/employees, satisfaction, etc.)
- **Regulatory** – compliance with state privacy/security requirements, FERPA, 800-171, Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standards (PCI DSS), etc.

Table of Contents

Resources

- **Cobit 5 – comprehensive for information security principles, policy and framework**
  - APO 13 Manage Security and other areas

- **ISO 27001- Information Security Management System (ISMS) – an overarching management framework**
  - 27002 – outlines hundreds of potential controls which may be implemented
  - 27003 – provides guidance on implementing ISMS
  - 27004 – covers information security management measurements and metrics
  - ***ISO/IEC 24760-1 A framework for identity management—Part 1: Terminology and concepts***
  - ***ISO/IEC CD 24760-2 A Framework for Identity Management—Part 2: Reference architecture and requirements***
  - ***ISO/IEC WD 24760-3 A Framework for Identity Management—Part 3: Practice***
  - ***ISO/IEC 29115 Entity Authentication Assurance***
  - ***ISO/IEC WD 29146 A framework for access management***
  - ***ISO/IEC WD 29003 Identity Proofing and Verification***
  - ***ISO/IEC 29100 Privacy framework***
  - ***ISO/IEC 29101 Privacy Architecture***

Resources (continued)

- **NIST**
  - Standards – SP 800 – 37, 53a, 60, 70 Special Publication
  - 800-63-3: Digital Authentication Guideline
  - Identity systems management program - http://www.nist.gov/itl/idms/index.cfm
  - Computer Security Resource Center - http://csrc.nist.gov/projects/iden_ac.html
  - NIST SPECIAL PUBLICATION 1800-9 – Access Rights Management for Financial Services
  - The attribute-based access control (ABAC) model https://csrc.nist.gov/News/2018/NIST-Researchers-Publish-Book-on-ABAC

Resources (continued)

- **The white papers…**
  - CapGemini – Identity and Access Management
  - Gartner – various whitepapers and webinars
  - Webinars
- **Health IT – ONC**
  - SAFER Guides - https://www.healthit.gov/safer/
  - How to Identify and Address Unsafe Conditions Associated with Health IT
- **Cloud Security Alliance – 12 domains identity and access management**
- **NACD – National Association of Corporate Directors**
  - 2017 Cyber Risk Oversight http://boardleadership.nacdonline.org/Cyber-Risk-Handbook-GCNews.html
- **OCEG (Open Compliance and Ethics Group) – Audit Access Control**
  https://go.oceg.org/illustration-audit-ready-access-control

Table of Contents

Conclusion

- **Need to audit**
- **Need to have the right audit scope**
- **Need to review key systems and supporting infrastructure**
- **Recommendations need to address root cause**
- **It is not an IT problem – Key success for safety, cyber security, protection of intellectual property, and strategic initiatives… and do not forget efficiency…**

Table of Contents

Questions?

How to Contact Us

- **For questions please contact:**

- **Johan Lidros**
  - Johan.lidros@emineregroup.com
  - w (813) 832-6672 x9101
  - c (813) 355-6104

Ongoing IT Governance Updates

- **Interested in on-going IT Governance and IT Security updates?**
  - Sign up for our weekly newsletter “RiskIT “at www.emineregroup.com

UPCOMING ACUA EVENTS

ACUA 2018 Annual Conference
Sept 9-13, 2018
New Orleans, Louisiana