Auditing Identity & Access Management: Addressing the Root Causes

HCCA – Compliance Institute
April 18, 2018
Johan Lidros CISA, CISM, CGEIT, CRISC, HITRUST CCSFP, ITIL-F
President Eminere Group

Table of Contents

• Introduction
• Current Environment
  ▪ IT / Systems
  ▪ AHIA Survey
  ▪ Audit Approach and Key Findings
• Root Causes
• Best Practice – Identity and Access Mgmt (IAM)
  ▪ Processes
  ▪ Measurements
• Proposed Audit Approach IAM
• Resources
• Conclusion
• Q&A
Presenter

- Johan Lidros, Founder and President of Eminere Group
- Has provided information technology governance and information security services in the healthcare industry 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

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?
Introduction

- **Session Objectives:**
  - Objective 1: Best practice in access management
  - Objective 2: How to audit 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

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 organization's success?
  - Patient Safety
  - Operations
  - Financials
  - Intellectual Property
  - Patient Communication/Satisfaction
  - Cyber risk
  - Recruiting the best (physicians, nurses, etc.)
  - ...

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, etc.)
Table of Contents

- Introduction
- Current Environment
  - IT / Systems
  - AHIA Survey
  - Audit Approach and Key Findings
- Root Causes
- Best Practice – Identity and Access Mgmt (IAM)
  - Processes
  - Measurements
- Proposed Audit Approach IAM
- Resources
- Conclusion
- Q&A

Typical Environment - Healthcare

- ~200 – 1000 “systems”
- How do we define systems?
  - OS and servers (unix, windows)
  - Databases
  - Applications
  - Mobile Apps
  - Network devices
  - Utilities and Tools – job scheduling systems, source code repository, virtualization (Vmware), firewalls, routers, sharepoint, others?
  - Medical Devices
  - Etc.
- What do you currently audit?
  - Application layer
  - Database layer
  - OS layer
RESULTS FROM THE AHIA 2015/2016/2017 HEALTHCARE IT AUDIT AND INFORMATION SECURITY STUDY

Info Security Top Risk Areas

- SIEM and log management: 70.0%
- Biomedical devices: 60.0%
- Application log management: 50.0%
- Encryption management: 40.0%
- Social media: 30.0%
- Meaningful Use compliance: 20.0%
- PCI 3.0 compliance: 10.0%
- Disaster recovery/business continuity: 5.0%
- Mobile device management: 0.0%
- Outsourced (cloud-based) services: 0.0%
- Virtual security (e.g., VMware): 0.0%
- Identity and access management: 0.0%

11

12
IT Audit Top Risk Areas

Question 1 What is your most critical System?

???
Question 1 What is your most critical System?

A. EMR
B. Financial System
C. Pharmacy
D. Lab
E. PACS
F. Password/Encryption key vault

Question 2

If access reviews are performed, for what percentage of your systems are reviews performed?
### Scope of Access Reviews 2016

For what percentage of your systems are reviews performed?

![Bar chart showing the percentage of systems with access reviews performed.]

<table>
<thead>
<tr>
<th>Percent</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>All systems (100%)</td>
<td>44.8%</td>
</tr>
<tr>
<td>75% to 99%</td>
<td>10.3%</td>
</tr>
<tr>
<td>50% to 74%</td>
<td>10.3%</td>
</tr>
<tr>
<td>25% to 49%</td>
<td>3.4%</td>
</tr>
<tr>
<td>1% to 25%</td>
<td>27.6%</td>
</tr>
<tr>
<td>None</td>
<td>2.8%</td>
</tr>
<tr>
<td>I don’t know</td>
<td>0.0%</td>
</tr>
</tbody>
</table>

### Question 2 2017

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

<table>
<thead>
<tr>
<th>Answer Options</th>
<th>Response Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>All systems (100%)</td>
<td>2.8%</td>
</tr>
<tr>
<td>75% to 99%</td>
<td>16.7%</td>
</tr>
<tr>
<td>50% to 74%</td>
<td>8.3%</td>
</tr>
<tr>
<td>25% to 49%</td>
<td>5.6%</td>
</tr>
<tr>
<td>1% to 25%</td>
<td>38.9%</td>
</tr>
<tr>
<td>None</td>
<td>5.6%</td>
</tr>
<tr>
<td>Do not know</td>
<td>22.2%</td>
</tr>
</tbody>
</table>
Question 3

If access reviews are performed, for which type of systems and accounts are they completed? Please select all that apply.

<table>
<thead>
<tr>
<th>Answer Options</th>
<th>Response Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial systems</td>
<td>77.1%</td>
</tr>
<tr>
<td>Electronic medical record systems</td>
<td>74.3%</td>
</tr>
<tr>
<td>Biomedical systems</td>
<td>22.9%</td>
</tr>
<tr>
<td>Lab systems</td>
<td>34.3%</td>
</tr>
<tr>
<td>Pharmacy systems</td>
<td>34.3%</td>
</tr>
<tr>
<td>Radiology/Imaging systems</td>
<td>31.4%</td>
</tr>
<tr>
<td>Enterprise access control system (e.g., Active Directory)</td>
<td>51.4%</td>
</tr>
<tr>
<td>File and folder permissions</td>
<td>14.3%</td>
</tr>
<tr>
<td>Administrative accounts</td>
<td>42.9%</td>
</tr>
<tr>
<td>Service Accounts</td>
<td>31.4%</td>
</tr>
<tr>
<td>Cloud-based applications</td>
<td>11.4%</td>
</tr>
<tr>
<td>Not applicable</td>
<td>8.6%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td></td>
</tr>
</tbody>
</table>

Other (please specify)
**Question 4 - What is your organization’s standard minimum password length?**

<table>
<thead>
<tr>
<th>Answer Options</th>
<th>Response Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 8 characters</td>
<td>5.7%</td>
</tr>
<tr>
<td>Exactly 8 characters</td>
<td>57.1%</td>
</tr>
<tr>
<td>Between 9 and 12 characters</td>
<td>28.6%</td>
</tr>
<tr>
<td>More than 12 characters</td>
<td>8.6%</td>
</tr>
</tbody>
</table>
Question 5: How frequently does your organization require passwords to be changed?

<table>
<thead>
<tr>
<th>Answer Options</th>
<th>Response Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Once a year</td>
<td>15.6%</td>
</tr>
<tr>
<td>Once every 6 months</td>
<td>28.1%</td>
</tr>
<tr>
<td>Once every 90 days</td>
<td>56.3%</td>
</tr>
<tr>
<td>Once a month</td>
<td>0.0%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td></td>
</tr>
</tbody>
</table>
Question 6:

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

<table>
<thead>
<tr>
<th>Answer Options</th>
<th>Response Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>For all users</td>
<td>15.2%</td>
</tr>
<tr>
<td>For remote access only</td>
<td>51.5%</td>
</tr>
<tr>
<td>For privileged users only</td>
<td>0.0%</td>
</tr>
<tr>
<td>Have not implemented two-factor authentication</td>
<td>33.3%</td>
</tr>
<tr>
<td>Other (please specify)</td>
<td></td>
</tr>
</tbody>
</table>
Frequency of Access Reviews 2016

- No reviews performed: 7.7%
- Reviews performed sporadically: 30.8%
- Continuously: 11.5%
- Quarterly: 26.9%
- Semi-annually: 0.0%
- Annually: 23.1%

No established standard for frequency of access reviews

Typical 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?
Common IAM Audit Findings

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

- Terminated users still active
- The process to handle workforce changes...
- Password requirements
- Authentication requirements (2FA, Single Sign-on)
- Identification process
- Not a comprehensive repository of non-staff users (volunteers, student, physicians, etc.)
- Password storage (passwords in a file for service accounts?)
- Lack of formal procedures
- Lack of resources
- Lack of measurements
- Decentralized security – inefficient
Common IAM Audit Findings

- Others???

Table of Contents

- Introduction
- Current Environment
  - IT / Systems
  - AHIA Survey
  - Audit Approach and Key Findings
- Root Causes
- Best Practice – Identity and Access Mgmt (IAM)
  - Processes
  - Measurements
- Proposed Audit Approach IAM
- Resources
- Conclusion
- Q&A
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
    - Resource intensive too fix
      - Not enough resources
      - Don’t have the right resources
    - Not a ‘priority’ – how do you balance fixing security issues vs addressing business or clinical related needs?

Root Causes

- 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
- Tool Support for IAM
  - Implementation
  - Wrong tool
- Resources/prioritization
- No or limited IAM program
- …. 
Table of Contents

- Introduction
- Current Environment
  - IT / Systems
  - AHIA Survey
  - Audit Approach and Key Findings
- Root Causes
- Best Practice – Identity and Access Mgmt (IAM)
  - Processes
  - Measurements
- Proposed Audit Approach IAM
- Resources
- Conclusion
- Q&A
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, etc.)
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.)
- HIT/HIE Architecture
- EHR system interoperability
- Consent directive (paper/electronic)
- Patient provides consent to share sensitive health information and HIPAA Permitted Uses and Disclosures

What is Computable Privacy?

- To achieve health, an individual’s electronic health data need to be digitally connected to their consent choices.
- Health care providers, and their health IT systems need to know what to do when the individual does not document a choice.
- Telemedicine, community health supports, and other innovative delivery processes will be stunted if we cannot make privacy computable.

Granular Choice

Basic Choice

Permitted Uses = Background Rules

This is HIPAA
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

<table>
<thead>
<tr>
<th>Type and Number of Systems</th>
<th>Trend</th>
<th>Goal</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHI</td>
<td>242</td>
<td>↓ 150</td>
</tr>
<tr>
<td>PII</td>
<td>312</td>
<td>↑ 250</td>
</tr>
<tr>
<td>Critical</td>
<td>85</td>
<td>↓ 75</td>
</tr>
</tbody>
</table>

| Number of FTE IAM | 4 | ← 6 |
| Number of Access Reviews | 52 (15%) | ↑ 80% |

<table>
<thead>
<tr>
<th>Number of Access requests</th>
<th>Initial</th>
<th>↑</th>
<th>change</th>
<th>←</th>
</tr>
</thead>
<tbody>
<tr>
<td>-Terminations</td>
<td>500</td>
<td>↓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Sample Key Measurements (cont.)

<table>
<thead>
<tr>
<th>Terminated Users</th>
<th>Trend</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Centralized Systems</td>
<td>↑</td>
<td>M</td>
</tr>
<tr>
<td>Decentralized Systems</td>
<td>↓</td>
<td>H</td>
</tr>
<tr>
<td>Cloud</td>
<td>↑</td>
<td>H</td>
</tr>
<tr>
<td>Appropriate Access</td>
<td>←</td>
<td></td>
</tr>
</tbody>
</table>
Table of Contents

- Introduction
- Current Environment
  - IT / Systems
  - AHIA Survey
  - Audit Approach and Key Findings
- Root Causes
- Best Practice – Identity and Access Mgmt (IAM)
  - Processes
  - Measurements
- Proposed Audit Approach IAM
- Resources
- Conclusion
- Q&A

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 Health Information Exchanges (HIEs)
- 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;
- **Security** - ensuring information security, integrity, and availability;
- **Patient Safety** – Improve risk management
- **Strategic** – ensure business alignment improve key strategic needs/initiatives (business partner initiatives, physician/patient satisfaction, etc.)
- **Regulatory** – compliance with the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standards (PCI DSS)
Table of Contents

- Introduction
- Current Environment
  - IT / Systems
  - AHIA Survey
  - Audit Approach and Key Findings
- Root Causes
- Best Practice – Identity and Access Mgmt (IAM)
  - Processes
  - Measurements
- Proposed Audit Approach IAM
- Resources
- Conclusion
- Q&A

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
  - 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
  - NIST SPECIAL PUBLICATION 1800-9 – Access Rights Management for Financial Services

- **The white papers…**
  - CapGemini – Identity and Access Management
  - Gartner – various whitepapers and webinars
  - Webinars

- **Health IT – ONC**
  - SAFER Guides - [https://www.healthit.gov/safer/](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**

- **OCEG (Open Compliance and Ethics Group) – Audit Access Control**
  - [https://go.oceg.org/illustration-audit-ready-access-control](https://go.oceg.org/illustration-audit-ready-access-control)
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 patient safety, cyber security and strategic initiatives.
# Table of Contents

- Introduction
- Current Environment
  - IT / Systems
  - AHIA Survey
  - Audit Approach and Key Findings
- Root Causes
- Best Practice – Identity and Access Mgmt (IAM)
  - Processes
  - Measurements
- Proposed Audit Approach IAM
- Resources
- Conclusion
- Q&A
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