Healthcare Industry Case Study

Security Guidance Matters

Executive Summary

Business Challenge

Eliminate duplication and adopt best practices for identity and access management and governance in a complex organizational and regulatory environment for a regional healthcare company.

Solution

A rationalization of people, processes, and technology with a comprehensive identity and access governance strategy.

- Current-state discovery
- Future-state blueprint
- Detailed 1-year project plan
- 3-year Roadmap

Benefits

Actionable information for the organization to make informed decisions on the appropriate investment and deployment strategy for their IAM solution framework. A complete solution designed to allow our client to secure ongoing investment to support an enterprise Identity and Access Management program.

Business Challenge

Meeting the demands of the evolving healthcare industry is an ongoing challenge. Healthcare systems are often very complex: legal, contractual, and regulatory relationships between provider associations, business partners, clinics and hospitals are difficult to handle simultaneously. It's difficult to feel confident that you can demonstrate compliance.

In addition to the environmental complexity, companies commonly rely on IT consultants or software vendors to provide expertise for projects related to subjects outside their core competencies. These projects types and problem domains vary greatly. They may range from departmental portals to enterprise-wide business intelligence to desktop support systems. Despite this variety, security is a concern that cross-cuts all these project types and problem domains. If an organization does not have a clear enterprise security strategy then project pressures can lead to one-off solutions to meet the needs of a particular initiative.

Our client had found themselves in exactly this situation. Over time multiple consultants for various projects prescribed technology as part of their solution. Identity and access management, security governance, etc., cut across various platforms and technical capabilities — without a clear enterprise strategy a consultant or a vendor may stand up a complete stack of technology that they are familiar with, but which duplicates functionality that already exists in other systems. While this may make sense for some targeted applications, in general it is not economically sustainable.

Make Your Strategy More than a Wish List

Identity ecosystems evolve under the pressures of business expectations, regulatory demands, and changing technology.

Business leaders expect IT to simplify experiences and reduce both time and cost of administration. Eliminating needless duplication is a must.

Users expect corporate systems to work as smoothly and seamlessly as consumer tools. One account to use everywhere, self-reliance, and seamless access.

Demonstrating that users have only appropriate and intended privileges is a high-stakes problem. Show your regulators and auditors you have your house in order.

Achieving these objectives while reducing cost and improving quality presents a serious challenge. *That's where Clango excels.*

We help you build a coherent identity and access management strategy with achievable milestones towards your long-term goals. We work with you to set priorities that match your business objectives, building the business case and financial models you need to deliver the right results.

Clango Engagement

For an organization to be able to cost-effectively scale, it must be able to leverage common systems and services to provide enterprise capabilities to the business. To do this it needs to shift from a systems perspective to a capability perspective. Our engagement provided a comprehensive view of not only the technology our client had, but the people and processes that were needed to deliver a particular capability.

Analysis

- Reviewed existing IAM capabilities throughout the infrastructure, including exceptions and workarounds, gaps, and duplication of processes.
- Comprehensively evaluated not only the technologies our client had, but the people and processes that were needed to deliver a particular capability.
- Defined lifecycle management using an entitlement chain based on user communities. This means the stronger business relationship a user has with the organization (e.g. employee) the more access they have to resources, the less directly connected relationship they have, may warrant access to fewer resources.

Solution Evaluation

- Determined the encompassing capabilities needed to align information technology with strategic business drivers.
- Evaluated solutions that take into consideration the internal and external forces (e.g. government regulation, NSTIC, etc.) affecting the evolution of Identity and Access Governance.
- Identified strengths and weaknesses of the current Identity and Access Governance infrastructure and how that could be complimented with additional technology to achieve sound governance.

Are you interested in becoming a reference?

Contact Information

Email: info@clango.com

Phone: 651.259.1001

Follow the Conversation

www.clango.com

www.facebook.com/clangoinc

Results Achieved

- Identified areas of transformation which requires improvements in organizational structure, IT roles, and oversight over the enterprise; recommended de-duplication of processes and retiring in-house developed application by centralizing access rights provisioning, access certification, and provisioning of resources using COTS.
- Identified the weaknesses and strengths of the current Identity and Access Management software and how that could be complemented with additional technology to achieve governance and compliance to regulation.
- Identified a sound and practical approach to building an Identity and Access Governance infrastructure that the organization can handle based on their capabilities and business drivers.
- Defined lifecycle management using roles and an entitlement chain based on user types. This means that the more business relationship you have with the organization, (e.g. employee) the more access you have to resources, the less relationship you have with the organization, the less access you have to resources.
- Provided the necessary milestones for Identity and Access Governance starting with the implementation of a blended ITIL and COBIT Framework, Governance starting with entitlement catalog, Provisioning starting with the evaluation and data cleanup of the many sources of records; Self-service and credential synchronization to improve user experience, and the implementation of Privileged Account Management to mitigate risks resulting to data loss.