Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

Insurance | the way we see it

Enterprise Governance Risk & Compliance: Enhancements for Health Payers

People matter, results count.

Table of Contents

1. Summary

This paper focuses on strategies to improve the management of functional IDs for health payers. We review a recent project for a leading U.S. health payer and assess how functional IDs are currently managed, look at associated risks, and recommend steps to gain a future state that strengthens existing information technology governance risk and compliance frameworks.

Like most large companies, the health payer has grown through acquisitions over the years. During that time, the company acquired IT assets and adopted different governance models which have led to a lack of standardization and uniformity across the IT framework. This has led to IT handling issues in different ways through multiple processes that are sometimes counter-productive. A recent audit required the health payer to make high remediation expenditures to address audit findings. The insurance company estimates it spends an average of $18 million on IT security projects per year.

2. An Introduction to Functional IDs

A functional ID (FID) is a generic account used for an IT asset. This ID can be used by users such as testers or processes such as automated batch jobs. These IDs are classified as shown in the table below.

To help keep functional IDs in check, many IT organizations use a repository to store the FID, certification and owners. Others require individual IT asset owners to maintain a list of functional IDs under their control. Since functional IDs are different from IDs used for application or database related activities, it becomes easy to confuse application IDs with other FIDs, especially in mainframe environments where cryptic mainframe login IDs are in use.

2.1. What are common problems with functional IDs?

The health payer in this example did not have a repository. While some asset owners had a list of FIDs under their control, there was no systematic process to organize and track FIDs for the organization. This resulted in a few problems:

- No visibility on the number and functionality of FIDs
- Lack of accountability on the use of FIDs
- Risk of interactive FIDs being used for malicious activities such as disrupting systems, unauthorized updates, and data leakage or corruption
- FID passwords were shared, written down and hard-coded which increased the risk of misuse and unauthorized disclosure of sensitive data including protected health information or pricing

Exhibit 1. Classification criteria for functional IDs

Design	Static A default ID that was packaged and pre-programmed in the IT asset by the original vendor. Generally, these cannot be modified	Non-static An ID that was created outside of the normal software development lifecycle for commercial off the shelf packages. Generally this ID can be created, modified or deleted during the software lifecycle.
Use	Interactive An ID that allows a user to assume its identity and inherit all privileges that were granted to the FID	Non-interactive An ID that does not allow a user to assume its identity
Entitlement	Privileged An ID that has elevated entitlements at par with the entitlements of a system administrator or super user	Non-privileged An ID with minimal rights necessary to perform the intended functions

2.2. How to Document Functional IDs

The first step in managing FIDs is to document them. We recommend a regulated process to create IDs through a security request system.

For example, a health payer can maintain effective control over FIDs by storing them in a central repository which captures:

- FID network or system ID
- FID owner including title, division and department
- Application or system associated with the FID. This information includes the application or system inventory number, owner and operating environment
- Interactive status
- Privilege status
- Static/non-static status
- Detailed information on the purpose of the FID
- Password location

3. How to Secure Functional IDs

Given the diversity of IT assets at most insurance companies, it's impossible to set up a 'one size fits all' approach for securing FIDs. We recommend the following criteria to ensure FID security.

3.1. Define owners

All FIDs must be owned by a full-time employee even if the requestor is a contractor or vendor. It's good practice for each FID to have a technical and functional owner who are different individuals and do not have a direct reporting relationship. The technical owner is responsible for the maintenance of the FID from a systems and application perspective while the functional owner is responsible for the FID from a business perspective. Their responsibilities are shown in the following table.

3.2. Set provisions

Provisioning is the process of requesting and granting appropriate access to a FID based on the requestor's role and responsibilities. The requestor should be given the rights that are required to perform daily or predefined activities based on their need. Often companies provide too many or too few permissions because the requestor's requirements aren't clearly understood.

To help a health payer set provisions, Capgemini created a FID request form that captures key information related to the request and use. The data populated on this form synchronizes, upon approval, with the FID repository. When FIDs are created outside of the request form process, they are entered into the FID repository to ensure that an up-to-date inventory of FIDs is kept at all times.

3.3. Manage passwords

Although sharing passwords is a violation of enterprise security standards, sometimes the same FID is used by several authorized users. To improve security for interactive FIDs:

Exhibit 2. Responsibilities of the technical and functional owners

Technical owner	• Ensures that the FID is appropriately provisioned on local and remote system • Assesses the impact of code or other technical changes on the functionality of the FID • Ensures that FID documentation in the central repository is accurate and up-to-date
Functional owner	• Ensures that the FID is appropriately provisioned on local and remote system • Assesses the impact of code or other technical changes on the functionality of the FID • Ensures that FID documentation in the central repository is accurate and up-to-date

- Passwords must not be shared
- Passwords must not be hard-coded in clear text
- All passwords must expire in accordance with the company's password expiration policy.
- FID passwords must be stored in an encrypted password repository
- The password repository must have a secure checkout process which does not divulge the password

3.4. Register inventory

Updating the inventory for FIDs should be extracted from an insurer's "golden source(s)" of information, for example Oracle Identity Manager, Tivoli Identity Manager, or others. If the insurer has unconnected interfaces for ID management, it's essential that the company implement a secondary interface to help identify and distinguish FIDs that are created and/or provisioned outside the normal processes.

Another avenue for updating FID inventory is through the use of an existing tool such as SeviceNow. A typical implementation may involve updating service offerings in ServiceNow to include the following:

- **Application Functional ID – Create.** Request creation of a new application FID. The creation process captures the required artifacts for FID inventory
- **System Functional ID – Create.** Request creation of a new application FID. The creation process captures required artifacts for FID inventory
- **Application Functional ID – Terminate.** Request termination of an application FID
- **System Functional ID – Terminate.** Request termination of a system FID
- **Application Functional ID – Update.** Update pertinent data for an application FID
- **System Functional ID – Update.** Update pertinent data for a system FID

3.5. Review entitlements

All privileged and interactive FIDs must have entitlements recertified based on a pre-defined schedule. The recertification should be performed by the functional owner of the FID since he or she is closest to the business. To simplify the process, the functional owner can recertify all individuals with access at the same time.

3.6. Automate maintenance

Maintaining FIDs can be extremely time consuming in certain business areas. To simplify the process, automatic logic can be applied so all FIDs that have not been used on provisioned systems in a set period of time can be automatically flagged for deactivation. All active FIDs that are updated up to 90 days before the recertification date can be automatically tagged as recertified.

3.7. Log audits and review requirements

For all interactive privileged functional IDs, companies must log activities and report to information security or other similar organizations for daily review. Any malicious activities should follow existing response processes defined by the company.

4. Functional IDs & Data Security Tool

In response to an audit, a health payer needed to monitor databases containing a predefined population of personally identifiable information and protected health information. We helped the insurer deploy a commercial tool to monitor access to these databases. In the near future, the health payer plans to expand the population of the databases to be monitored and extend the tool's functionality to block access and mask sensitive data. The masking and blocking functionality will be rule-based using rules that are programmed into the tool based on data collected from current monitoring activities.

For monitoring purposes, users for the data security tool are classified into four broad areas:

- **Privileged users** are generally database administrators
- **Authorized users** are regular day-to-day users like business analysts that frequently have a business need for direct access to databases
- **Trusted users** are synonymous to FIDs.
- **Suspicious users** are those who do not belong to one of the other user categories

Monitoring rules may vary among databases. Some databases with comprehensive monitoring have rules configured to log all activities by trusted users while other databases may ignore trusted users.

After all FIDs are documented as discussed in the last chapter, it's imperative that data security monitoring rules be updated to log activities of FIDs in concert with privileged or authorized users based upon the entitlements of the FID.

5. Privileged Accounts Policies

Since some of the recent breaches of information in the healthcare industry were due to comprised credentials of privileged accounts, insurers should implement generic policies for all privileged accounts in addition to securing FIDs. We recommend:

- No privileged account can have a shared password that is known to more than one person
- Passwords of all privileged accounts are kept in a password vault
- Passwords of privileged accounts should be randomly generated for each use (One-time password).
- Activities of all privileged accounts be logged and the logs monitored daily.
- Restrict interactive logons for privileged accounts.

6. Conclusion

The proliferation of functional IDs in general computing environment is a necessary evil. Recent breaches of secure, high availability, and sensitive information-containing systems, though not all involved FIDs, generally involved use of compromised credentials of privileged accounts.

To protect themselves from an array of cyber attacks and crimes and tighten up loose ends in security, insurers should take pragmatic steps to protect FIDs. Better protecting FIDs will enable health payers to quantify risk, provide an avenue for integration into the security program, and create business opportunities for internal organizations to deliver a high return on investment.

Capgemini has successful executed FID projects across a number of regional and global insurance companies. We have strong relationships with world class partners like HP and IBM and a proven track record of providing data and cybersecurity services:

- **Applications security**, including digital forensics and penetration/ vulnerability testing
- **Endpoints security** such as office terminal, smart phone, PLC, or tablets
- **Identity and access management** including ID lifecycle management, privileged user management, and risk-based authentication
- **Data centers security** including defense in depth, architecture zoning, segregation of networks, hardening and configuration of IT products, and security architecture for virtualized data center
- **Consulting** and audit services
- **24/7 monitoring** services
- **Encryption** for data at rest and in transit

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

www.capgemini.com/insurance

About the Author

Imran Khan is a Senior Consultant in the Global Insurance practice for Capgemini's Financial Services business unit. Since joining Capgemini in 2014, Imran has implemented IT solutions for North American insurance companies. He is based in New York.

Prior to Capgemini, Imran worked on risk management systems for leading financial institutions including Citigroup and Capital One. He holds a BS in Management Information Systems from University of Houston-Clear Lake.

Learn more about us at: **www.capgemini.com/insurance**
or email: **insurance@capgemini.com**

About Capgemini

Now with 180,000 people in over 40 countries, Capgemini is one of the world's foremost providers of consulting, technology and outsourcing services. The Group reported 2014 global revenues of EUR 10.573 billion.

Together with its clients, Capgemini creates and delivers business, technology and digital solutions that fit their needs, enabling them to achieve innovation and competitiveness.

A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

Learn more about us at
www.capgemini.com

People matter, results count.