What is a data security framework?

[[](https://www.google.com/search?sxsrf=APq-WBv0CUAY73CGQbH5n2DqnF70O4_now:1648607667481&q=What+is+a+data+security+framework?&tbm=isch&source=iu&ictx=1&vet=1&fir=hC4KeOsDd6AT9M%252CHRXUoRABAq7aGM%252C_&usg=AI4_-kTylcwjNN10UgSRVaAzlZJVhin8ZA&sa=X&ved=2ahUKEwigqJOT5uz2AhU1D0QIHfv7BLcQ9QF6BAg_EAE#imgrc=hC4KeOsDd6AT9M)](https://www.google.com/search?sxsrf=APq-WBv0CUAY73CGQbH5n2DqnF70O4_now:1648607667481&q=What+is+a+data+security+framework?&tbm=isch&source=iu&ictx=1&vet=1&fir=hC4KeOsDd6AT9M%252CHRXUoRABAq7aGM%252C_&usg=AI4_-kTylcwjNN10UgSRVaAzlZJVhin8ZA&sa=X&ved=2ahUKEwigqJOT5uz2AhU1D0QIHfv7BLcQ9QF6BAg_EAE" \l "imgrc=hC4KeOsDd6AT9M)

What is an IT security framework? An IT security framework is **a series of documented processes that define policies and procedures around the implementation and ongoing management of information security controls**. These frameworks are a blueprint for managing risk and reducing vulnerabilities.

Encryption of Data Communication

For the Transport Layer, we are planning to use SSL/TLS using Asymmetric encryption scheme. We will be using a dedicated Hardware Security Module to store Cryptographic keys. A 1024 bit RSA key is proposed to be used for key exchange and AES (Rijndael) key strength will be 256 bits. The System will be certified for FIPS 140-2 compliance.

Security Strategy

The general strategy for the whole application suite is

* SSL/TLS for transport level encryption
* SAML based SSO between modules
* Tivoli based Identity/authorization solution
* Digital signature for anti-tampering
* Hardware Security Module for Key Storage
* PCI based encryption for Credit cards
* Full Table encryption for DB2 and SQL server
* Future support for Multi-factor Authentication

Logging, Security and Auditing

Content routing & filtering

Message level validation

Data Security framework

Security testing

Physical and electronic threats

Adaptive data security

SoftLayer Security Services

Simply building a fence between infrastructure, environment and malicious activity isn’t a guarantee of safety. True security leverages proven methodologies for safeguarding an environment (and the physical facilities that host it) from the ground up and constantly updating those measures as the threat landscape changes.

SoftLayer has a multi-level approach for shielding customers against physical and electronic threats, with comprehensive practices and a range of options for Physical and Operational, Network, System, Application and Data Security. SoftLayer Managed Hosting assesses customer needs and collaborates with the customer to create the optimal security strategy for locking down your environment while providing flexibility for peak performance.

SoftLayer’s security procedures utilize industry best practices from sources including The Center for Internet Security (CIS), Microsoft, and Red Hat and more.

All SoftLayer data center facilities are SOC 2 certified.

**Features**

* SOC 2 Compliant
* 24/7 physical security of data centers and Network Operations Center monitoring
* Integrated server hardening
* Regular full-system virus scanning and systems patching
* Regular security profile review and recommendations

SecurityLayer Services

IT infrastructure requires multiple, overlapping tiers of security for its total protection. This is the driving principle of SoftLayer’s multi-level security strategy for shielding against physical and electronic threats—SecurityLayer® Services.

Through certified operational procedures and practices, a comprehensive range of software and hardware security solutions, and strategic partnerships with industry-leading companies, SoftLayer helps maximize uptime, protect private information and mitigate business risk

Digital Signature

When a citizen uploads a document, he has to digitally sign it using his private key. The document will be verified by using OpenSSL library’s Digital Signature module.

Security Architecture

On Demand Security Arch

Figure 1.4.2.3-2: On Demand Security Architecture.

The Logical architecture which we are following is based on IBM consulting’s Tivoli practice endorsed On Demand Security Architecture (refer *Figure 1.4.2.3-2*).

Security Level Management

A Security Level Management (SLM) will be put in place by UST consulting’s (COBIT/ITIL certified) security professionals which broadly comprises of

* Defining the Security Level
* Data Analysis based on logs and audit trails
* The Current Security Analysis based on empirical facts
* Closing the gap by preventive measures

Security Procedures and Policies

Being a secured infrastructure UST consulting’s Standard Operational Procedure (SOP) for secured systems will be applied. Samples of aspects covered are

* Network Access Control
* Security logs
* Physical Security
* Cryptographic Parameters
* Password Policies
* User Account Policies
* Security Incident handling
* Computer System Usage Policy
* Device Management and Security

PCI Compliance

The System will compliant to PCI DSS standard version 2.0. A check list of items which we are planning to implement is given below. It has got correspondence to PCI 2.0 compliance rule.

* A firewall configuration to protect cardholder data is present
* Preclude usage of vendor-supplied defaults for system passwords and other security parameters by enforcing it
* Cardholder data is stored in a secure hardware device
* SSL/TLS Encrypted transmission of card holder data between systems.
* Malware protection for Systems running in the Realm
* Secure System and Application coding practices.
* Restrict access to cardholder data by business need-to-know
* Assign a unique ID to each person with computer access
* Restrict physical access to cardholder data
* Tracking/monitoring all access to network resources and cardholder data
* Regular test of security systems and processes
* A constantly maintained policy that addresses information security
* Fortigate® Security Appliance
* FortiGate 300 series security appliances provide high performance and enterprise-class firewall protection. Customers also get direct access to FortiGate's native management tools, extending complete, granular control over advanced firewall and security features.
* Anti-Virus and Anti-Spyware Protection
* McAfee® security products add an additional layer of security. Anti-Virus protection can be added at no additional charge, or McAfee Total Protection is available for protection against Viruses and Spyware.
* SSL Certificates
* The Symantec and GeoTrust brands are backed by a dedication to excellence in customer support. Every SSL Certificate from a Symantec-owned company is signed with a reliable and ubiquitous root so customers don't have to worry that they will end up with Web site visitors not protected by their SSL Certificate because there is a problem with the underlying SSL root.
* Two-factor Authentication
* Add even more protection to a SoftLayer Customer Portal login with external, two-factor authentication. The extra layer of security shields the account from unverified access to ensure that servers, data, and account are always safe. Symantec Validation and ID Protection provide a dynamic security code that can be used in addition to a user name and password for safe and secure account access. PhoneFactor provides out-of-band authentication via phone call, SMS message, and mobile apps.

Physical and Data Security Practices

SoftLayer has a multi-level approach for shielding customers against physical and electronic threats, with comprehensive practices and a range of options for Physical and Operational, Network, System, Application and Data Security. SoftLayer Managed Hosting assesses customer needs and collaborates with the customer to create the optimal security strategy for locking down their environment while providing flexibility for peak performance. SoftLayer’s security procedures utilize industry best practices from sources including The Center for Internet Security (CIS), Microsoft, and Red Hat and more. All SoftLayer data center facilities are SOC 2 certified.

Storage and Backup Services

SoftLayer’s comprehensive selection of storage and backup services provides multiple technologies, allowing customers to select the ideal level of security, reliability, and flexibility for their environment and applications. Every type of data does not have to be backed up the same way. Some type of data may be backed-up multiple times a day, while for others, once a week might be enough. Our recommended schedule and strategy includes:

* Full Backups: Weekly, all file systems and databases
* Incremental Backups: Daily, all file systems and databases
* Offsite Storage: via snapshot transfer for iSCSI volumes, including volumes used for storing non-snapshotted NAS backups and database backups, retention near-online for 1-3 months, periodic restore/verify at least monthly

Monitoring and alerting

Security layers: Enterprise 🡪 network 🡪 data

Security patch management

Layers of data types

**Preventing Unauthorized Releases of Data**

SoftLayer makes use of multiple layers of network security including stateful firewalls. In addition, SoftLayer IaaS provides support for clients to provision shared or dedicated firewalls and load balancers as well as fortinet application security appliances allowing for the construction of secure multitier topologies.

SoftLayer event logs are always active and protected from unauthorized access. Significant events (including login attempts, privilege escalations) are logged and analyzed. SoftLayer platform does not have access to client data.

SoftLayer security logs are not externalized for client use. Appropriate information is collected in SoftLayer platform logs that allow for analysis, identification and audit of the platform.

SoftLayer regularly monitors and analyzes security logs generated from platform componentry for irregular suspicious activities. Logged alerts are handled in a timely manner - and, if applicable information is communicated to the client via the standard incident response and support mechanisms.

A support and incident response system exists to communicate any activity to clients regarding the SoftLayer infrastructure. If SoftLayer detects malicious network activity, it will null route the traffic and work with the client to remediate the activity. If not remediated in 24 hours SoftLayer maintains the capability to take the target IP address offline. SoftLayer provides the capability for clients to provision and configure network and application level firewalls. The logs from these devices that protect the subscribed resources are available to the client.

Access Privileges

Team UST will closely monitor access privileges and in accordance with policies and standards defined in the City of LA’s Information Security policies. Overarching policies include the following requirements:

* Formal administration process that requires manager level authorization for all users to the database and supporting utilities will be defined.
* Sensitive database utilities (e.g., load utilities) will be restricted to personnel responsible for the maintenance of the databases.
* Establish Database Security administration procedures for:
  + Documented authorization for database access capabilities including input and verification of security related maintenance.
  + Requirement to retain access request forms for not less than 2 years.
  + Periodic review and monitoring of user access capabilities.

Security

Security policies and standards must be in accordance with policies and standards defined in the City of LA Information Security policies.

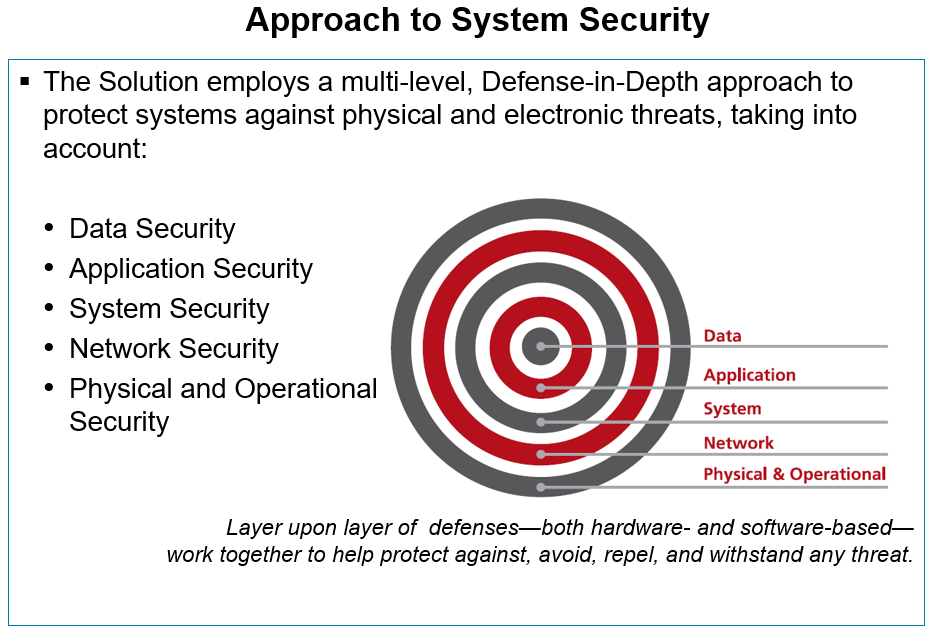
Changes & Modifications

Team UST DBA will maintain the database using the following procedures:

* Allocating sufficient system storage for the application database
* Adding, altering, and deleting users, roles, and privileges
* Periodically defragmenting and compacting the database for more efficient operation
* Upgrading database software and associated applications, as necessary
* Providing routine backup of the database
* Maintaining an approved list of valid values for data consistency
* Maintaining redundancy control to ensure that each data record is unique and consistent with conventions
* Performance and Tuning
* Recovery

Handling sensitive information in the test environment provides the following advantages:

* Securing sensitive information from misuse, either within or outside the organization – by removing all identifying information
* Compliance with federal laws
* Allows restricting access to production data and using the test environment for all testing purposes
* Working from a locked copy minimizes the chance of data corruption in the production environments
* Overall reduction in complexity versus implementing encryption/decryption in the production environment to support test access



++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

Business Value of Data Management

**Services** -

* Data Archival
* Test Data Management (Data Subset)
* Data Mask (de-identification)

**Challenges**

* HR data size ~950 GB
* Finance data size ~1.5 TB
* Data Management cost too high (time, cost, personnel)
* Payroll takes a long time
* Annual membership enrollment takes a long time
* The cost is too high
* Sub production environment takes too much storage
* Sub production data volume costs too much
* Data refresh takes too long
* Strain on networks
* Every release is delayed
* Code quality is low

* No meaningful data masking/de-identification

**Solution**

* Archive/shred older data based on policies
* Use data storage type based on data usage type, e.g., operational data on SSD, inactive data on network storage, old but still required (7-10 years old) data on magnetic tape
* Subset data to create test data baseline that is representational of the entire data set
* Mask (de-identify) test data to preserve PII

**Cost**

* Initial Total cost $435,050
* Ongoing cost $???/year

**Benefits**

* The right amount of data for the right environment (how much data for each environment?)
* Savings to management due to smaller data set size (how much savings?)
* Payroll get processed in much shorter time window (how much time savings?)
* Annual membership enrollment process streamlined (1. how time it saves, 2. how many fewer people it takes, 3. how much money it saves, 4. how much new business it generate, 5. how much goodwill it generates?)
* Data refresh takes less time (how much time savings?)
* Sub production requires much smaller storage (what are the storage savings?)
* Lower sub production storage requirement yield savings (how much savings?)
* Improved production release (how much time savings it will yield? How personnel savings it yields?)
* Improved code quality – quicker and easier data refresh enables shorter test cycles and will enable more testing in the same timeframe (how much code quality it will improve?)

* Comply with PII regulations (*need to look externally for how much fine is PII violations? penalties under criminal and civil statutes and laws*)

**Process**

* **Learn what the data archival policy is based on regulatory requirements**
* **Collect data archival policy definitions**. For example -
  + Active Data - still active and less than 3 years old
  + Inactive Data - between 3-5 years data
  + Archived Data - 5-7 years old data
  + Historical Data - 7-10 years old data
  + To be shredded data - older than 10 years data
* Identify Master data (Master data will not be archived) and its size
* **Based on the data archival policies, calculate the size of data for each definition (category)**
  + Active Data size - ??? (*Note: Master data size will also be considered part of Active Data*)
  + Inactive Data size - ???
  + Archived Data size - ???
  + Historical Data size - ???
  + To be shredded data size - ???
* **Determine the storage type**
  + Active Data - it should be the high performance storage, e.g., SSD or SAN
  + Inactive Data - It can be stored on NAS (but still online)
  + Archived Data - It can be stored on NAS (it can be offline, unless there is a need for it for reporting)
  + Historical Data - It can stored on magnetic tape (the cheapest option)
  + To be shredded data - This should be shredded
* **Calculate the storage cost**
  + Current Data Storage Cost = current storage size \* the price of current storage type

* Active Data Cost - size of active data \* the price of selected storage type
* Inactive Data Cost - size of inactive data \* the price of selected storage type
* Archived Data Cost - size of archived data \* the price of selected storage type
* Historical Data Cost - size of historical data \* the price of selected storage type

* Add up all the above costs and subtract it from the Current Data Storage Cost
* **Create baseline data for sub production environments**
  + Determine the maximum amount of data required for any environment. For example, performance testing environment will require the most data, since it is expected to be as close to production as possible. But it should not exceed 50%; the projected results can be extrapolated.
  + Subset data representing all scenarios, e.g., 50%
  + Mask (de-identify) the subset data. This will **establish a test data baseline.**
* **Serve all sub production environments from the baseline test data**
  + Development environment - 10% of baseline data
  + Integration environment - 20% of baseline
  + QA environment - 30% of baseline
  + Performance environment - 100% of baseline
  + UAT environment - 30% of baseline
  + Training environment - 30%
* **Calculate the savings**
  + Add up the current storage consumption for all sub production environments
  + Add up the new, trimmed total storage consumption from all sub production environments
  + The delta of the two will give you the savings in terms of size and cost

* Labor cost saving can also be calculated from the storage delta (most simplistic form, e.g., does not factor in the cost of time spent on configuration of data subsetting and data masking. But, the effort is mostly upfront. During subsequent runs, this effort is minimal)
* The time savings will be calculated from -
  + The current time to prepare (data loading and data masking) all sub production environments - The new time to prepare (data subsetting and data masking will be based on configurations. Also, the data masking is done only once per refresh cycle) all sub production environments (this can be extrapolated from the size difference)
  + Decrease the test cycle (add up time savings for all sub production environments)
* Better code quality - more agile/nimble test data management will enable more repeated testing at a much lower cost in time and money. According to industry analysis, it could yield as much as 30% improved code quality
* Shorter runtime for backup and recovery. This can be calculated by subtracting the to time to backup and recover the new data set size from the time it takes to backup and restore the current (full) data set size. For example, if the current data set takes 4 hours to backup and the after the archive, the new data set size is only 70% of the original data set size, the backup will only take 2 hours and 48 minutes
* **Annual Enrollments**
  + Current budget for annual enrollment (*need to get it from the business or whichever entity owns the budget*)
  + Current duration to validate annual enrollments (*Note: the only savings will be realized are via new and improved test data management, the rest of the activities will remain the same; Note: if there are multiple enrollments drives a year, we need to add all up*)
  + If annual enrollment validation is conducted in a separate infrastructure, the cost reduction of the lower infrastructure demand will also be factored in
  + The annual enrollment validation cost will be calculated based on the percentage of time spent on validation from the current budget for annual enrollment
  + New annual enrollment validation cost will be based on duration and infrastructure to validate annual enrollments
* **Payroll process improvement**
  + This can be calculated based performance improvement based on trimmed data set size
  + Shorter processing window, since backups will only take a fraction of the time (*current backup time - the backup time for the trimmed data set size after the archive*)
* ***Recommendation: Use Excel sheet for data tables and calculations***
* **Value Addition**
  + Documentation of the data relationships
  + Improved understanding of the current data models
  + New insights to data assets for additional opportunities
  + Performance improvements will yield from having CRUD thru smaller data set. (Experience has shown that the performance improvements can be anywhere between 10% - 30%)

**Items needed from UST personnel working on HR and Finance systems at WellPoint**

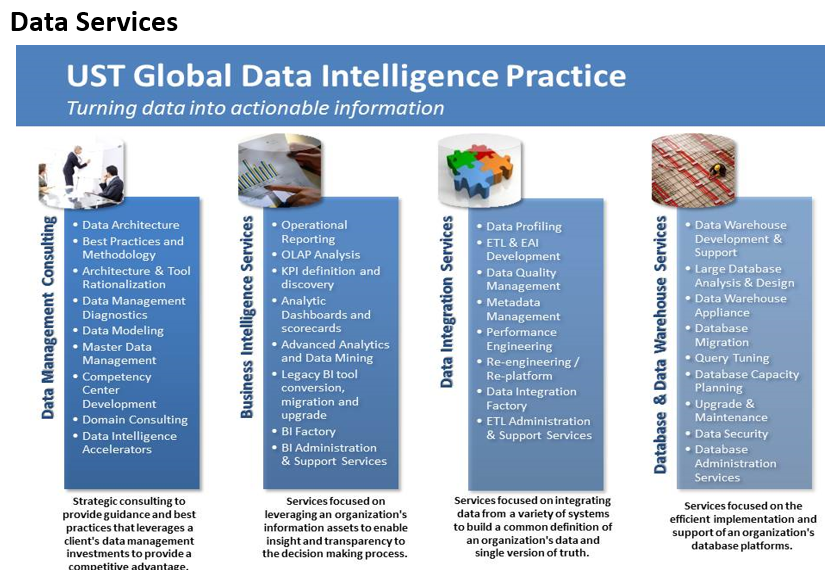
* **Data archival policies and regulatory requirements.**
* **Data archival policy definitions**. For example -
  + Active Data - still active and less than 3 years old
  + Inactive Data - between 3-5 years data
  + Archived Data - 5-7 years old data
  + Historical Data - 7-10 years old data
  + To be shredded data - older than 10 years data
* Master Data identification and size
* **Data size by archival policies**
  + Active Data size - ???
  + Inactive Data size - ???
  + Archived Data size - ???
  + Historical Data size - ???
  + To be shredded data size - ???
* **Current storage type**
* **Quality of data**
  + Is data referential integrity enforced in the database and documented reasonably well
  + Or, is it enforced thru the code? If so, could we get those relationships documented?
  + Is there a lot orphan data? (*Note: an attempt should made to establish its relationship(s), if unable to rectify, a management decision should be secured and act accordingly. Recommendation - this data should be archived to the Historical Data*)
* **Data refresh technology** – what technology is being used today to refresh data in sub production environments
* **IBM Optim Usage** (*Sujith Madhusoothanan might be able to help with this*)
  + Did WellPoint ever use IBM Optim for the Test Data Management in the Finance and HR business units?
  + If so, what were the reasons they stopped using it?
  + Data Masking
    - Are there any tools being evaluated at WellPoint currently?
    - If so, which ones and the findings?
* **UST/WellPoint**
  + Annual Enrollments budget
  + Duration to setup annual enrollments (configurations)
  + Duration to validate annual enrollments (testing)
  + Duration to implement annual enrollments (implementation)
* **Payroll process**
  + Current duration to process payroll
  + Consequences of delayed payroll processing
* **PII Violations**
  + Financial penalties accrued (avg. $7.2M)
  + Criminal and legal penalties levied

++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

Policy based Data archival

Data masking

Data obfuscation



Adaptive security

Differentiator

Value-adds

Data Security standard

Policies

Access controls

