CS-GY6863 Fundamentals of Information Security Management

Final Report:

Skyline: Information Security Strategy

Suvetha Kannan, sk5897@nyu.edu
Tatiana Polunina, tp1094@nyu.edu
Hadjer Benkraouda, hb992@nyu.edu
Masato Anzai, ma3156@nyu.edu

Executive Summary

Information Security Strategy is designed to protect information assets from a wide range of threats, to ensure business continuity and minimize business risk. Information Security has to be robust to address an evolving array of threats. This Strategic plan identifies strategies and solutions which accomplish Skyline's Information Security's goals.

The information security program structure is defined carefully through recommendations given in the NIST standard as well as some of the organizational models that were developed by our major competitors. The security program features organizational structure along with the training program. The SETA program will be developed catered to the organization's needs ranging from the general user to the technical users. The information security structure also features the operating model as well as the regulatory frameworks such as FINRA and Cybersecurity information sharing act that must be implemented into the organization's operating model.

An inclusive Contingency plan was devised that follows the NIST standard and consists of four main components. The first is Business Impact Analysis to identify critical to our organization business processes, information assets and business units. Threats were prioritized, analyzed on STRIDE-DREAD models, threat agents were identified. Followed by an Incident Response plan that includes a detailed protocol of "During the Incident", "After the Incident" and "Before the Incident". Next, a Business Resumption plan was drafted, that features two components: Business Continuity plan and the Disaster Recovery plan that help the company resume to its full potential. Finally the Contingency testing plan was set.

Skyline follows the NIST Risk Management framework and we calculate the risk based on the quantitative and qualitative risk analysis process. Skyline also has the Information Security Policies in place including the Enterprise Information Security Policy, Issue Specific Security Policy and the System Specific Security policy. The basis for the Continuous Monitoring process in Skyline is the NIST CAESARS framework. Skyline has two SIEM tools integrated with each other and they are ArcSight and Splunk. Skyline also follows strict third party vendor management structure to ensure utmost security. This is done by third party vendor screening and profiling to hand pick the best suppliers and then continuous monitoring to ensure compliance.

Another important aspect that was explored is Identity and Access management of skyline's data and resources. A IAM structure adhering to NIST standards was put in place and a system using Passwords, Biometrics and ID cards was implemented for easy, efficient and accountable access of information and resources.

As a technically driven corporation that thrives to keep up with the technical standards of the industry, a cloud implementation is needed for flexibility, cost effectiveness, and scalability. The cloud security structure will also follow the NIST recommendations given for Cloud Computing. Some of the key features that must be identified for proper cloud security implementation is a continuity plan/incident response plan. The challenges of cloud computing will be covered as well as the possibilities of blockchain technology implementation.

In the face of growing prevalence of mobile devices, new Mobile Device Security Strategy was defined. New BYOD policy was developed and outlined, threats to mobile devices identified and Central Mobile Device Management solution proposed to be implemented following NIST recommended five-phase Life Cycle.

Table of Contents

Introduction

Skyline recognizes that it is imperative to its success and mere survival to manage, control and protect information assets. Given the nature of Skyline's business, our company is a target to various security challenges and threats, which are constantly growing in number, diversity and sophistication. As new trends and technologies emerge there have to be mechanisms protecting business infrastructure, assets and systems.

The aim of this document is to develop, implement and maintain an effective Information Security Strategy, adequate for the growing number of threats and decentralized nature of our organization, which will promote and facilitate our company's goal of being one of the top global Investment Management organizations over the next thirty six months.

Current State

Our organization is a global Investment Management company. It manages financial assets such as shares, bonds and real estate for private and corporate investors. The investments that Skyline manages are multi-million dollar deals. Skyline has been successful in the past few years and has expanded to become a global company that has its international branches in New York, London, Singapore, Tokyo, Shanghai, San Antonio, Mumbai. To manage all information pertaining to the global clients and all the companies international branches Skyline has employed data centers in San Antonio, London, and Philippines.

Skyline's Mission - to position our company as one of the top ten Investment Management organizations in the world with a digital centric business model at its core within the next three years.

Skyline's Vision - Lead the industry by being the investment management firm of choice.

Skyline's Values - Innovation, Quality, Integrity

Business Direction

Skyline's strategic business objectives are outlined below. They are founded on existing global trends and support our company's mission.

- **Digital Innovation** - Research and Development initiative to create a digital centric business with focus on IoT. Develop new business models with enhanced platforms to achieve overall corporate success

- **Global Expansion** - Acquire successful startups to improve the buy/sell side research in the investment markets and determine the areas of investment

- **Cybersecurity** - Increase investments, improve the existing security models and protect against data loss and data breaches occurring in the organization

- **Cloud Solutions** - Research and consider moving some of the non-confidential information and systems into the cloud, creating a hybrid datacenter/cloud environment

The focus of Information Security Strategy will be on the following priorities:

Data Loss Prevention - Intellectual Property and research data are highly confidential and vital to our company's success. CISO's vision is to lay the groundwork for a long term DLP plan.

Identity Access Management - Categorization of the user access based on the access level required. For example, the user access provided for a system admin should not be the same for a normal user.

Physical Security - Skyline has ID card system privilege based access to its sites. We plan to make it more robust and implement monitoring

Proactive Management - Any ad hoc risks that may emerge should be counted for, thought about and if the management faces a new issue, a standby solution should be immediately put in place. (Ad Hoc Risk Committee will be responsible for this action)

Information Security Program Structure

There are several variables that can determine the structure of an Information Security Program. The simplest variables that determine the contents of an Information Security Program consists of organizational culture, size, and security capital budget.

As an organization that takes pride in technical prowess, a cyber security program is a sector that must receive full investment. The company can be categorized as a very large sized organization with major branches internationally. Given these attributes, the organization will propose 5% of the organization's total capital for the development of the Information Security Program.

Before creating a proper structural overview of the cyber security program's employment needs, the necessary information security functions must be acknowledged.

Table 1. Information Security Functions

Risk Assessment	Identifies and evaluates the risk present in IT initiatives and/or systems
Risk Management	Implements or oversees controls to reduce risk
Systems Testing	Evaluates patches used to close software vulnerabilities and acceptance testing of new systems to assure compliance with policy and effectiveness
Policy	Maintains and promotes InfoSec policy across the organization
Legal Assessment	Maintains awareness of planned and actual laws and their impact, and coordinates with outside legal counsel and law enforcement agencies
Incident Response	Handles the initial response to potential incidents, manages escalation of actual incidents and coordinates the earliest responses to incidents and disasters
Planning	Researches, creates, maintains, and promotes InfoSec plans
Measurement	Uses existing control systems to measure all aspects of the InfoSec environment
Compliance	Verifies that system and network administrators repair identified vulnerabilities
Centralized Authentication	Manages the granting and revocation of network and system credentials for all members of the organization
Systems Security Administration	Administers the configuration of computer systems
Training	Trains general staff in InfoSec topics, IT staff in specialized technical controls, and internal InfoSec staff in specialized areas of InfoSec, including both technical and managerial topics
Network Security Administration	Administers configuration of computer networks
Vulnerability Assessment	Locates exposure within information assets so these vulnerabilities can be repaired before exploitation

Functions that will be developed for our information security program can be categorized in four different areas:

1. Functions performed by business units outside the IT area of management:
   - Legal, Training
2. Functions performed within the IT group outside of the InfoSec area:
   - Systems Security Administration, Network Security Administration
3. Functions performed within the InfoSec unit as a customer service:
   - Risk Assessment, Systems Testing, Incident Response
4. Functions performed within the InfoSec unit as a compliance enforcement obligation:
   - Policy, Compliance/Audit, Risk Management

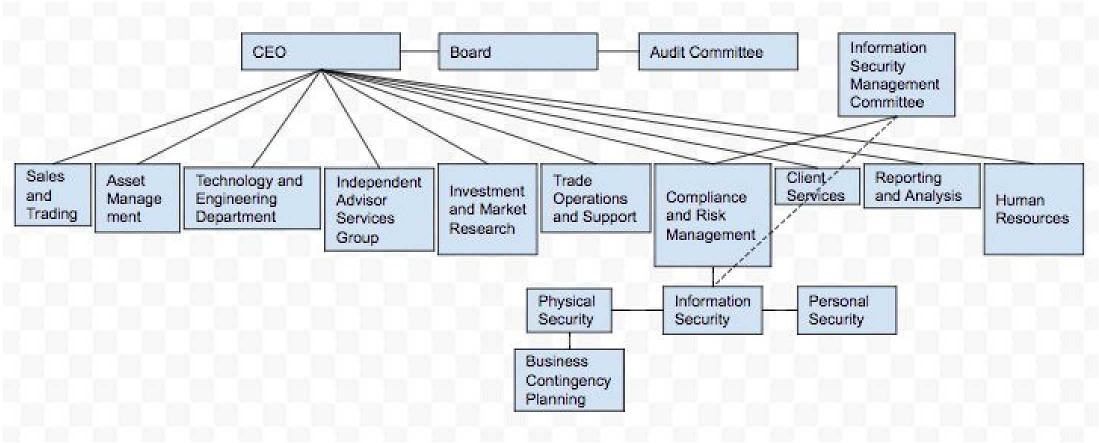
All of the functions will be performed within the company not only by the Information Security unit.

Information Security within the Organization

The Information Security Department can report directly to the Compliance and Risk Management Department. The Information Security Manager will report to the Chief Risk manager or the CRM. This approach allows a centralized perspective, prioritizing and comparing all risks across the organization. This is the most desirable option for an investment management organization.

Because the CISO will report to the CRM and the CEO, it allows for a better overall view of the corporation in a business oriented manner. Instead of limiting the capabilities of the Information Security Unit from misunderstanding the important business assets of the corporation, the cyber security unit will be able to better understand and mitigate business risks at a higher proficiency.

Figure 1. Skyline's Organizational Structure


CEO
Board
Audit Committee
Information Security Management Committee
Sales and Trading
Asset Manage ment
Technology and Engineering Department
Independent Advisor Services Group
Investment and Market Research
Trade Operations and Support
Compliance and Risk Management
Client Services
Reporting and Analysis
Human Resources
Physical Security
Information Security
Personal Security
Business Contingency Planning

Given the structure of the overall organization the next step would be to configure the Information Security Roles.

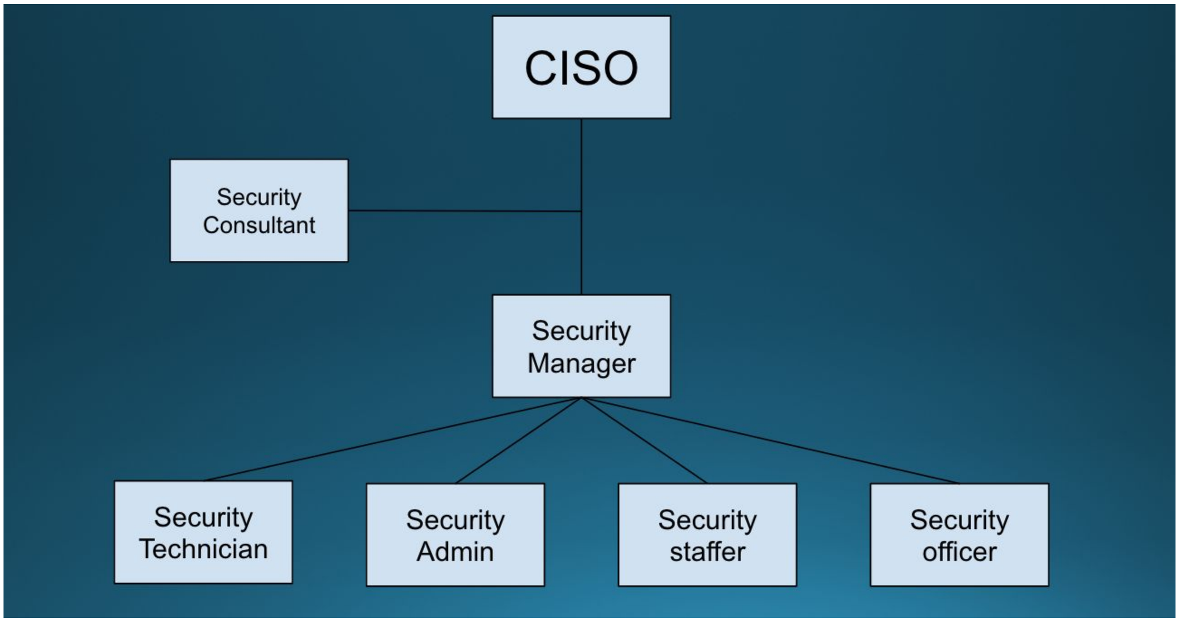
Information Security Roles

Information security positions can be classified into one of three types:

- Those that define
- Those that build
- Those that administer

The roles that will be implemented are: CISO, Security Managers, Security Technicians, Security Admins, Security Staffers, and Security Officer/Investigators

Figure 2. Information Security Roles



Information Security Education

The Security Education, Training, and Awareness program (SETA) will be implemented. The SETA will be customized for different members of the organization by:

- Functional Background:
  - General User - ex: human resources, financial analyst
  - Technical User - ex: Network Security Admin, System Admin
- Skill Level:
  - Novice
  - Intermediate
  - Expert

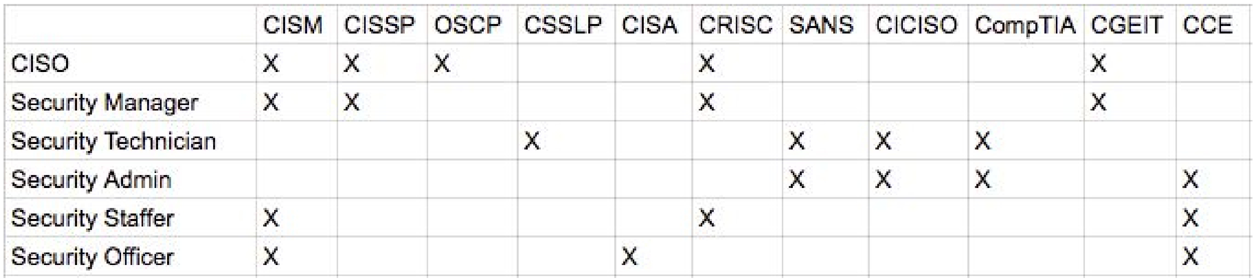
General Users

All users will go through a formal class to learn about the policies of the organization. There will be technical training such as password management, specialized access controls, and violation reporting. Social Engineering attack awareness will be emphasized through organizational media. New users will learn about security at orientation. A voluntary gamification program will be provided for all users to maintain and train for security. This gamification program will feature feedback and rewards for users who decide to participate.

Technical Users

Technical users require a much more in depth knowledge of security, especially the security team. Certain certification requirements will be employed.

Table 2. Certification requirements



	CISM	CISSP	OSCP	CSSLP	CISA	CRISC	SANS	CICISO	CompTIA	CGEIT	CCE
CISO	X	X	X			X				X	
Security Manager	X	X				X				X	
Security Technician				X			X	X	X		
Security Admin							X	X	X		X
Security Staffer	X					X					X
Security Officer	X				X						X

Information Security Operating Model

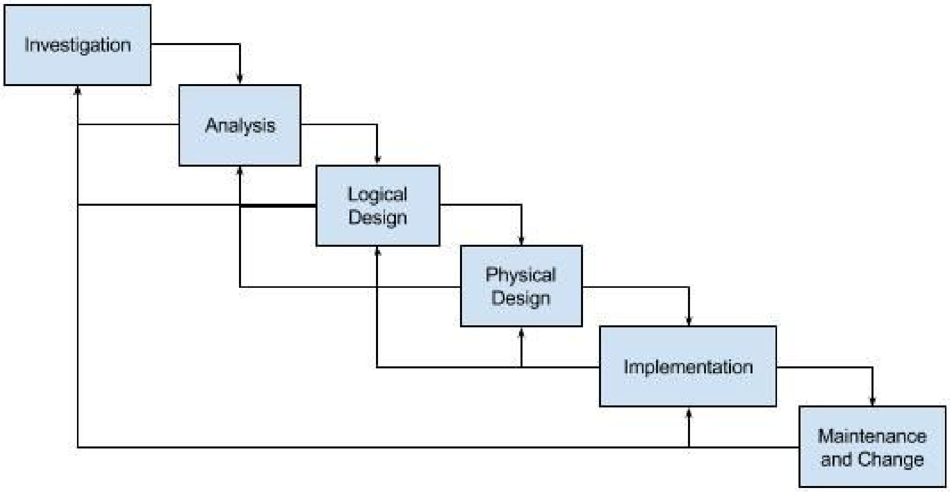
Regulatory frameworks will be put in place with regulatory policies for the organization to meet the standards set.

NIST Framework for Cyber Security Standards
FINRA - Skyline meets the standards set by FINRA and also meets PCI DSS.
GLBA - Financial Institutions Customer privacy act of 1999.
Cybersecurity Information Sharing Act - Threats faced by organizations similar to Skyline will be shared in a central repository and processing this data will help avert similar threats/attacks.
ISO/IEC 270001:2005 Standards

SecSDLC

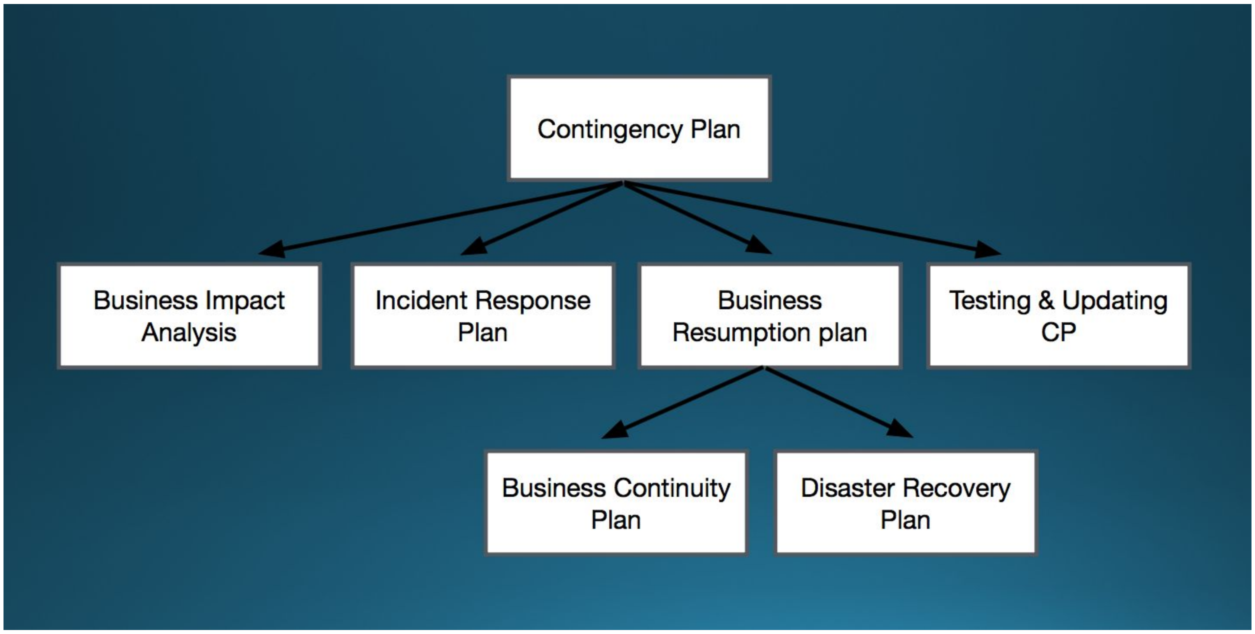
SecSDLC or Secure Secure Software Development Lifecycle will be used for the implementation of security application development.

Figure 3. SecSDLC



Contingency Planning

Figure 4. Contingency plan



As shown in Figure 4 the Contingency Plan (CP) at Skyline follows the NIST standard and consists of four main components. The first phase is Business Impact Analysis, followed by detailed Incident Response plan. Next, the contingency plan has to have a Business Resumption plan, which usually features two components: Business Continuity plan and the Disaster Recovery plan. The last component in the contingency plan is the testing and updating phase, which is very important as it makes sure that the plan is up to standards, most efficient and doable within the time frame needed.

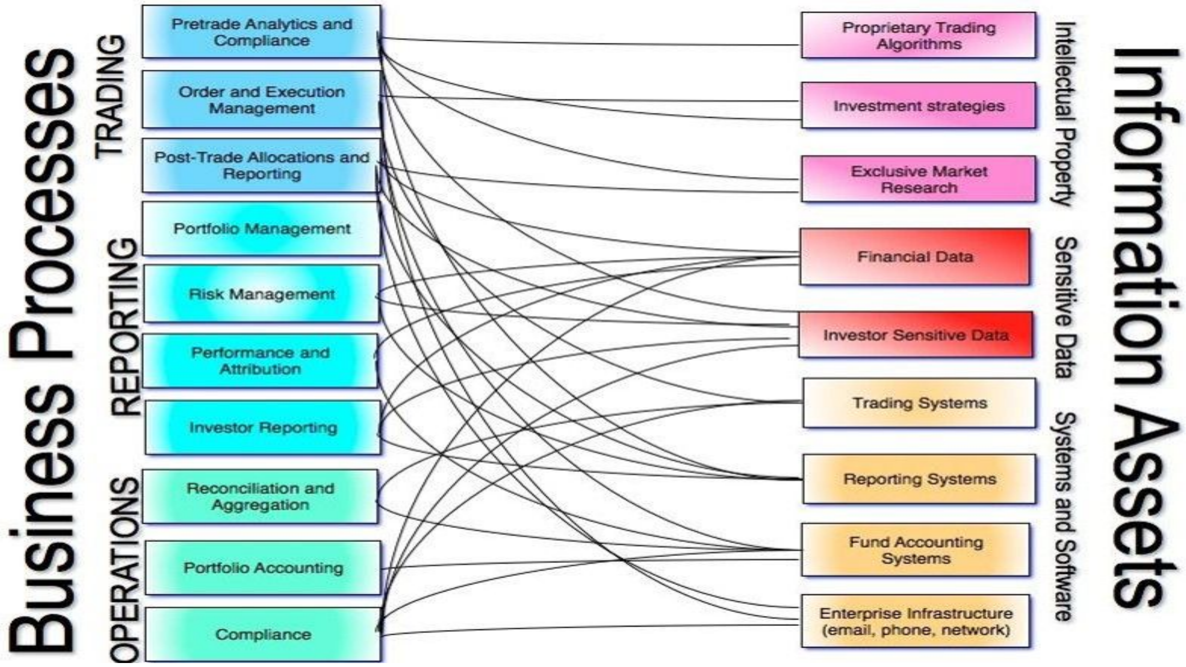
Business Impact Analysis

Critical Information Assets Identification

First step in identifying critical information assets is to determine the business processes which directly rely on data, systems and applications and would be impacted in case of a security breach affecting particular information asset.

Our main business processes can be divided into three groups: Trading, Reporting and Operations. Trading group business processes consists of Pre-trade Analytics and Compliance, Order and Execution Management and Post-Trade Allocations and Reporting. Business processes from reporting Group include Portfolio Management, Risk Management, Performance and Attribution and Investor Reporting. Operations processes are Reconciliation and Aggregation, Portfolio Accounting and Compliance. [1]

Figure 5. Business Processes and Information Assets



Respectfully our critical Information Assets can be divided into three groups:

- Intellectual Property, which includes Proprietary Trading Algorithms, Investment Strategies and Exclusive Market Research
- Sensitive Data, consisting of Financial Data and Investors' Sensitive Data
- Systems and Applications - Trading Systems, Reporting Systems, Fund Accounting Systems and Enterprise Infrastructure (email, phone, network, etc.)

Below is the list of business units, which are crucial to the survival of our business in the order of their priority:

1. Sales and Trading
2. Asset Management
3. Technology and Engineering Department
4. Compliance and Risk Management
5. Independent Advisor Services Group
6. Investment and Market Research
7. Trade Operations and Support
8. Client Services
9. Reporting and Analysis
10. Human Resources

Threat Attack Identification and Prioritization

Table 3 represents prioritization of Threats and vectors of Attacks.

Table 3. Threat Attack Identification and Prioritization

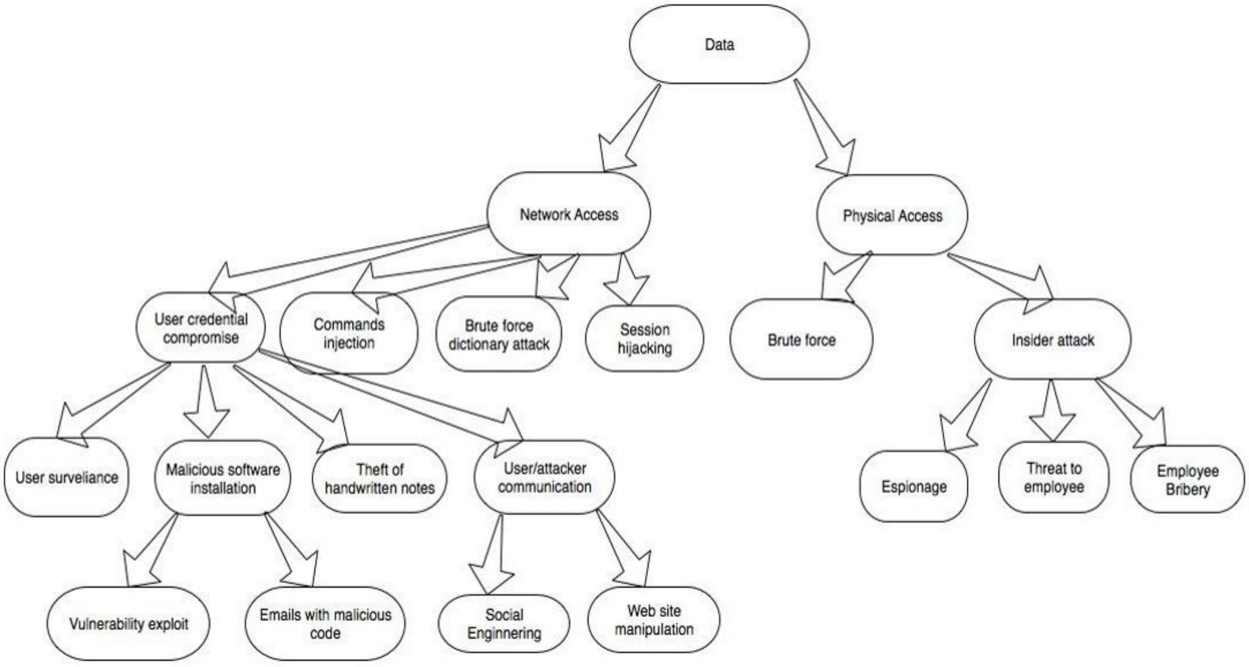
1	Compromises to intellectual property	Back doors in systems and applications
2	Deliberate acts of espionage or trespass	Insider information leakage
3	Deliberate software attacks	Malware infection, Brute force attack, Dictionary attack, Dos and DDoS, DNS cache poisoning
4	Deliberate acts of theft	Insider information offload
5	Acts of human error or failure	Social Engineering Attacks
6	Technological obsolescence	Outdated infrastructure at Philippines data center

7	Technical software failures or errors	Outdated infrastructure at Philippines data center
8	Technical hardware failures or errors	Disks, power supplies, cooling systems, server failures
9	Forces of nature	Fire, flood, earthquake, tornadoes
10	Deviation in quality of service from service providers	ISP and power outages

Given the nature of our business and how Intellectual Property is vital for our company's success, we consider its compromise as the biggest threat our organization faces. Since we rely on several third party software vendors (specifically our Trading and Reporting systems), a back door left deliberately or incidentally by Systems and Software Engineers represents the most probable vector of attack. Other threats to Intellectual Property include Deliberate acts of Espionage and Trespass, Deliberate acts of theft. Among the biggest threats are Deliberate software attacks and acts of human error or failure (due to their high probability and variety).

Figure 6 below represents an Attack Tree, where at the root lies our valuable Intellectual Property data . Multiple vectors represent paths for an attacker to get access, which can be either physical or network access. Each one of these vectors has to be considered and evaluated.

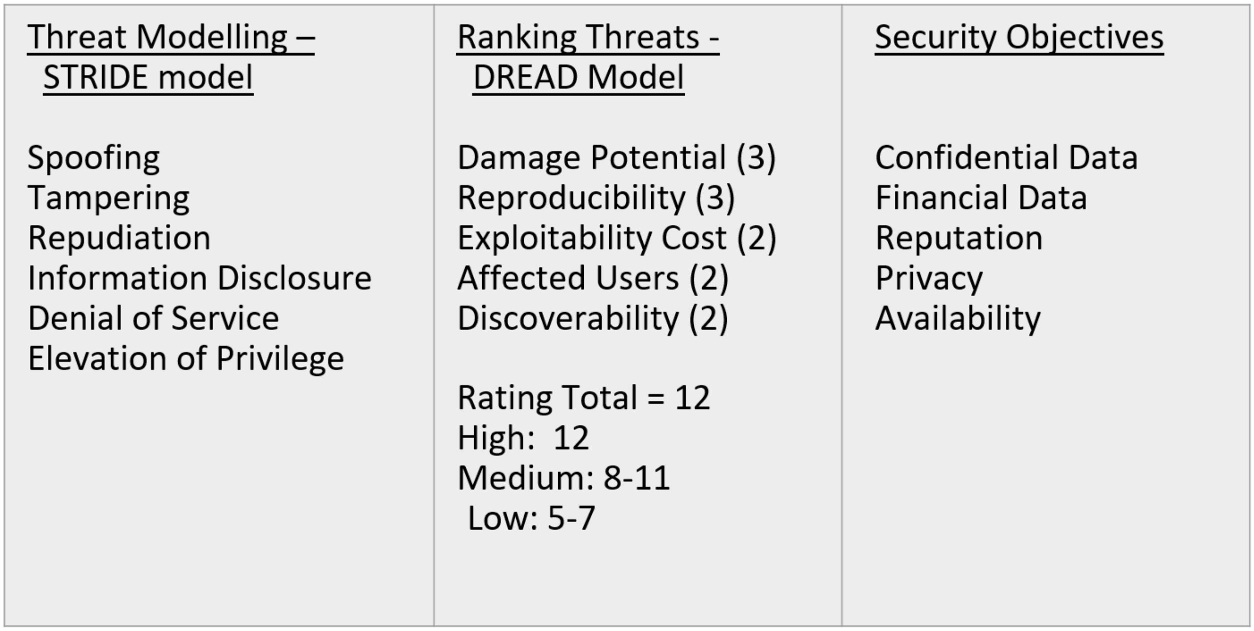
Figure 6. Attack Tree



Threat Modeling

We used a combination of STRIDE and DREAD models while conducting our threat modeling. When evaluating against STRIDE model we considered whether a threat is spoofing, tampering, repudiation information disclosure, elevation of privilege or a combination of those. Using a DREAD model we assigned numeric values to possible damage potential, reproducibility, exploitability cost, affected users and discoverability of threats. In addition we determined which Security Objectives will be targeted by each of evaluated Threats.

Table 4. STRIDE-DREAD Models



Threat Modelling – STRIDE model	Ranking Threats - DREAD Model	Security Objectives
Spoofing	Damage Potential (3)	Confidential Data
Tampering	Reproducibility (3)	Financial Data
Repudiation	Exploitability Cost (2)	Reputation
Information Disclosure	Affected Users (2)	Privacy
Denial of Service	Discoverability (2)	Availability
Elevation of Privilege		
	Rating Total = 12	
	High: 12	
	Medium: 8-11	
	Low: 5-7	

Using this type of analysis we determined that Software Attacks and Social Engineering/Human Errors scored the highest on our DREAD scale. Software Attacks also scored the highest on STRIDE scale along with Infrastructure Vulnerabilities. This Analysis will allow our company to determine the correct controls and produce effective countermeasures within budget.

Table 5. STRIDE-DREAD Threat Risk Modeling

Threat	STRIDE	DREAD	Security Objectives
Theft of Intellectual Property	I	Medium (9)	Confidentiality
Espionage or Trespass	T I	Low (6)	Privacy, Confidentiality
Software Attacks	S T R I D E	High (12)	C, F, R, P, A
Theft	T I	Medium (9)	Confidential & Financial Data
Social Engineering/ Human Errors	S T I E	High (12)	Confidentiality, Privacy

Infrastructure Vulnerabilities	S T R I D E	Medium (9)	Availability, Confidentiality
Software Vulnerabilities	S T I E	Medium (9)	Availability, Confidentiality
Hardware Failure	D	Low (5)	Availability
Natural Disaster	D	Low (7)	Availability
Backdoors from third party softwares	T D E	Medium(10)	C, F, R, P, A

The next type of Analysis we performed is Threat Agents identification. We considered what actors might target our Information Assets, what their motivation could be, what threat vector they might choose and how likely their attack to succeed.

Table 6. Threat Agents

Information Assets	Actors	Motivation	Threat Vectors	Capability
Proprietary Trading Algorithms	Competitors	Market advantage	Back doors, insider leakage, APT, Social Engineering	Medium
Investment Strategies	Competitors	Market advantage	Back doors, insider leakage, APT, Social Engineering	Medium
Exclusive Market research	Competitors	Market advantage	Back doors, insider leakage, APT, Social Engineering	Medium
Financial Data	Hackers	Financial gain	Back doors, APT, Malware, Brute Force Attack, Social Engineering	Medium
Investor's Sensitive Data	Hackers	Financial gain	Back doors, APT, Malware, Brute Force Attack, Social Engineering	Medium
Trading Systems	Hackers	Financial gain	Back doors, APT, Malware, Brute Force Attack, Social Engineering	High
Reporting Systems	Hackers	Financial gain	Back doors, APT, Malware, Brute Force Attack, Social Engineering	High
Fund Accounting Systems	Hackers	Financial gain	Back doors, APT, Malware, Brute Force Attack, Social Engineering	Medium

Infrastructure	Hackers, Competitors, adversaries, forces of nature	Market advantage, financial gain, vandalism	Back doors, APT, Malware, Brute Force Attack, Social Engineering, Outdated datacenter hardware and software, DoS and DDoS	High

We found that the highest variety of threat actors would target our Infrastructure amongst the rest of Information Assets. These threat actors have different motivation, might consider variety of threat vectors and the likelihood of attack success is high. As for our Intellectual Property, the most probable actors would be our Competitors, their motivation is Market Advantage and they would choose highly targeted threat vectors, such as application's back doors, insider espionage, advanced persistent threats and Social Engineering. We assigned medium capability to these actors due to very high cost of such attacks.

Incident Response Plan

The first step in creating a contingency plan is to create an Incident Response Team (IRT) that is trained to do incident detection, incident response and incident recovery. This team should also keep detailed documentation of previous incidents. The contingency plan accounts for these incidents and tries to prevents similar incidents in the future. To ensure that the best outcomes are reached detailed protocols are set for each stage of the incident, this is done by implementing Incident handling procedures for every incident. Documented in 3 steps:

1. Protocol "During the Incident". This describes procedures that are carried out at the time of incident. Includes delegates for each task Skyline's.
2. Protocol "After the Incident". This describes procedures directly following the Incident. This includes detailed procedure on how to to restore networks and systems.
3. Protocol "Before the Incident". This describes procedures preventing incidents, including regular backups, testing plans and training sessions.

Business Resumption Plan

As mentioned above, the business resumption plan consists of two components disaster recovery plan and Business Continuity Plan. At skyline we make sure that these plans are updated periodically and that they inline with the company's goals.

- Disaster Recovery Plan(DR): We Update Skyline's DR plan even unlikely events such as natural disasters. Skyline's DR plan also acts as a secondary safeguard in case the IR plan is unable to contain an incident.

- Business Continuity Plan: Skyline is a multi-million dollar firm. Although Skyline does everything possible to prevent incidents and disasters from happening it realizes that they might happen and that it has to be able to serve its clients and be able to run the most critical procedures.

Disaster Recovery Plan

The disaster recovery plan at skyline is developed in conjunction with the business continuity plan. This DR plan relies on the priorities and the recovery time objectives developed during the business impact analysis. Skyline’s disaster recovery plan is developed to restore hardware, application and data in time to meet the needs of business recovery. These objectives are satisfied through backups and redundancy.

Data Backups

The first step that we do at skyline is identified data on network servers, desktop computers, laptop computers and wireless devices that we need to be backed up this also includes other hard copy records and information. Our plan includes regularly scheduled backups from wireless devices, laptop computers and desktop computers to a our network server and data centers. Data on the server can then be backed up. Disk images of financial systems on servers in the company’s three data centers, where the disk images are stored, are taken. Replicas to these backups to the data centers are made for redundancy and then archived from disk to tape.

Redundant array of independent Disks(RAID) technology is used to ensures that the confidential data is backed. After this backing up of the backup is made to a cloud is done.

We also take into account backing up hard copy vital records by scanning paper records into digital formats and allowing them to be backed up along with other digital data.

Redundancy

Establishing redundant servers for all critical services and providing an alternate way to access the services and can still be interrupted is an essential component of an organization's disaster recovery planning. Having these redundant services in place at a secure, offsite location reduces disaster recovery time at skyline down to minutes rather than days.

As part of our redundancy initiative, services are synchronized to another site with backup servers to able to continue to perform services. Another important aspect of redundancy is having backup power supply. This includes generators or uninterrupted power supply (UPS) for critical process such as Stock related departments a backup power supply ensures that these processes run uninterrupted or with very little down time. Furthermore, we also include backup cooling systems that function in case the first ones fails, this ensure that the servers and other systems will not fail due to overheating.

Business Continuity Plan

After performing the risk assessment and management in the business impact analysis and setting safeguards to try to account for risks and prevent them, we develop a can to continue skyline's incase of disaster. Skyline has different types backup sites based on the different levels of criticality of each department.

Skyline understands the time sensitivity of its stock's related departments and therefore it has created a "Hot site" for these departments to be able to run, in the case of an incident or a disaster, with negligible downtime. The departments that are will be included in this site are Sales and Trading, Asset Management, Technology and Engineering. Next, For all its other client services, Skyline set up a "Warm site" that is able to run with a small down time. The departments that are will be included in this site are Independent Advisor Services Group, Investment and Market Research, Trade Operations and Support, Client Services, Compliance and Risk Management, Reporting and Analysis. Finally, for the rest of the company, in the case that the company isn't able to resume its function in the old site(earthquake that destroys the site) it relocates to this site for the non-critical departments. Skyline has multiple branches in New York, London, Singapore, Tokyo, Shanghai, San Antonio, Mumbai. The secondary sites are in case the Skyline branch experiencing the disaster can not delegate its functions to one of the other branches.

In addition to the of duty sites(Hot, Warm and cold) Skyline's business continuity plan also has a Mutual Agreement with Company X that provides either one of these companies with a backup site to run their business from until they can resolve the problem and move to the new site or even back to their old one.

Company X

Company X is a financial firm, Skyline has chosen it because it has similar equipment. This means that Skyline can get to work without having to add any equipment. Company X is not in the same geographical location as Skyline. This choice was made because if they are in the same physical location then they might endure similar natural disasters and therefore won't be able to serve as a backup site. Although Company X is also a financial firm it is a non competing company, Skyline made this decision because it wants to avoid the possibility of client/company data theft from the hosting company.

Testing/Updating Contingency Plans(CP)

The last part of the contingency plan is to test the aspects individually and then perform an overall test of the contingency plan. Throughout this process updates have to made to the contingency plan to ensure compliance with protocols and developments in the company. There are different tests and simulation that are performed in this stage. First is the desk check, in this test each employee alone. This is done when the CP is first drafted and after updates to it. Next, structured walkthrough take place, this has to be done with everyone involved in the CP after CP trainings. It is only done after lessons learned from Desk Check are added. The next step is performing simulations of the contingency plan. Since this is done individually it lies under employee duties and is done when the CP is first drafted and after updates. It is only done after lessons learned from Structured Walkthrough are added. After that parallel testing takes place, in this test all individuals involved in the CP plan act as if an actual incident has happened without halting the operation of the business. It is only done after lessons learned from Structured Walkthrough are added. This test has to be done biannually in Skyline. Finally, a full-interruption Test is done. During this test all the individuals involved in the CP plan act as if an incident happened including disrupting business tasks and performing all the needed steps that follow an incident. It is only done after lessons learned from Structured Walkthrough are added. Since this test is invasive and Skyline can not afford for its business to be halted very often this test will be done annually.

Risk Management

In Skyline, we are following the NIST Risk Management Framework which comprises of the below steps:

1. **Categorize** – The risks need to be categorized based on the level of impact of the risks such as High, Medium or Low.
2. **Select** – Based on the categorization, the Risk Management team chooses the baseline controls to mitigate the risk.
3. **Implement** – The chosen baseline controls are implemented and the security controls are documented.
4. **Assess** – After the proper implementation of the security controls, the operations are tested and are checked to determine if they produce the desired outcome.
5. **Authorize** – The Risk Management has to authorize the implementation of the security controls after determining the risk once the security controls are in place and checking if the risk is acceptable.
6. **Monitor** – The security controls that have been authorized and implemented are monitored continuously in the organization.

Risk Management Case Study

In order to understand how a particular business process could fit under the different risk management strategies, we worked on one business process that is critical to the functioning of the organization which is the “Infrastructure”.

1. **Risk Reduction** – In order to ensure that the Infrastructure should have reduced risk, we should ensure that the Infrastructure should comprise of standard, well – established products. For example, if we are planning on Installing new infrastructure products in the organization, installing a product that is well-established and which was launched a year ago is better than a product that was launched a few months ago. A well-established product will have more reviews and it will help us understand the risks in installing that product when compared to a newer product for which we do not understand the risks.

2. **Risk Mitigation** – In order to mitigate the risks, in Skyline we have our Disaster Recovery and the Business Continuity plans in place for the existing infrastructure along with the Incident Response Team.

3. **Risk Transfer** – In the case of the Risk Transfer, Skyline's Infrastructure is managed by Third Party Organizations.
4. **Risk Acceptance** – The risk will be accepted by Skyline if the cost of mitigating the risk is higher than the cost of the risk and also if the probability of the occurrence of the risk is very low. The value of Risk is calculated by using the below formula:
   Risk = Probability * Impact

Risk Analysis

There are two types of Risk Analysis:
1. Quantitative Risk Analysis (Objective)
2. Qualitative Risk Analysis (Subjective)

Quantitative Risk Analysis for Skyline

Asset – Investor's sensitive information
Case Study: If 5 investor's sensitive information is compromised with an average loss of $1 M due to a vulnerability in the application handling the investors information; in order to correct the vulnerability in the application, it will cost us $600000 to develop, test and deploy the applications and an additional $100000 a year as a maintenance cost for the application. The application needs replacement after 3 years.
Threat – Software Vulnerability
Likelihood of the occurrence of the event - Medium
Single Loss Expectancy (SLE) – $1 M
Annualized Rate of Occurrence (ARO) – 5
Annualized Loss Expectancy (ALE) – $5 M
Safeguard (S) = (600000/3) + 100000 = $300000
Annualized Net Benefit of Safeguard ANB (S) = ALE(without S) – ALE (with S) – ACS (S)

= \$5 000 000 – 0 - \$300000
= \$ 4 700 000 ~ 4.7 M
Positive value indicates that the safeguard is effective. Installing a security mechanism is an overhead when the
ANB(S) = 0 – ACS (S)
Therefore, the update to the application to fix the vulnerability needs to be done.
Quantitative Risk Analysis cannot be done for the rare events.

Qualitative Risk Analysis for Skyline

Similar to the above Quantitative risk analysis, we performed a complete analysis of the various business processed in Skyline that is critical to the operation of the organization and is tabulated as below along with the Qualitative Risk Analysis as High, Medium or Low.

Table 7. Risk Analysis

	Quantitative Risk Analysis	Qualitative Risk Analysis
Proprietary Trading Algorithms	>\$100 M	High
Investment Strategies	>\$10 M	Medium
Exclusive Market Research	>\$100 M	High
Financial Data	>\$150 M	High
Investor’s Sensitive Data (for 1 investor)	>\$1 M	Medium
Trading Systems	>\$10 M	High
Reporting Systems	>\$1 M	Medium
Fund Accounting Systems	>\$10 M	Medium
Infrastructure	>\$200 M	High

Information Security Policies

In Skyline, the security team already has a few information security policies in place. In this information security strategy, we are going to fine-tune the existing policies and also determine areas of improvement for the different types of information security policies.

Enterprise Information Security Policy (EISP)

In Skyline, we are working on an EISP to promote the collaborated research in the new business models by providing unrestricted access to resources for the required employees to perform quality research.

The existing EISP policies will be analyzed by the Skyline executives, business owners and the Incident Response Team.

We are going to establish a Policy Driven Information Systems Security Architecture and provide security awareness training to all the employees in the organization.

Establish timelines to detect, prevent and respond to security breaches.

The EISP is also subject to an annual compliance review and periodic review that occurs bi-monthly for the board to review the changes in the EISPs. The EISP also lists the responsibilities of the CEO, CIO, CISO and also the actions/review that is needed periodically.

Issue Specific Security Policy (ISSP)

The ISSPs are based on the business processes or the target areas of high risk based on which remediation efforts are used to create or modify the required policies.
There are three types of ISSP and they are:

1. **Individual Policy**
   An individual policy is created specific to a particular department in Skyline such as the Systems Management department.

2. **Comprehensive Policy**
   A comprehensive policy is a complete document of all the ISSPs specific to Skyline. With a comprehensive policy we keep track of all the ISSPs in the organization.

3. **Modular Policy**
   A modular policy is specifically crafted for a department in the organization. For example, Network Security breach policy crafted specifically for the network security/systems administration team with technology specific details.

System Specific Information Security Policy (SysSP)

The SysSPs are crafted based on the SOE (Standard Operating Environment) Guidelines and for each system SysSPs is crafted.

There are two types of SysSPs:

1. **Managerial guidance SysSPs**
   Example: Firewall Rule Configuration policy in Skyline with guidelines about how to configure the firewalls as well as the standards followed by the organization globally for consistency.
2. **Technical Specifications SysSPs**
   This type of SysSPs have details about the Access Control Lists with details about who, what, where, when and how with the read, write, execute and delete access they are provided.

Information Security Policies (Advisory/Informative)

The below table gives a complete set of details about the existing information security policies in the organization and the required modifications that are needed or if the existing information security policies will be replaced by the new information security policy.

Table 8. Security Policy

Existing Information Security Policies	Required Modifications/New Information Security Policies
Encryption Policy	Increase the existing key strength to better standards
Data Breach Policy	Additional Data Loss Prevention methods
Digital Signature Policy	Certificates and Certificate Authority Modifications
Remote Access	Multifactor Authentication using DUO/PingID
Software Installation Policy	Signature based verification for softwares

Mobile Device Encryption Policy	For email access on mobile devices, the mobile devices should be encrypted
Social Engineering Awareness Policy	Phishing and malware attacks

For example, the Software Installation Policy will have a modification to add that the softwares will be installed only after the signature verification of the software downloaded and the required hash value to verify the integrity of the software to be installed.

Threats and Policies

Table 9. Threats and Policies

Threats	Policies
Theft of Intellectual Property	Protection of Intellectual Property Policy (EISP)
Espionage or trespass by employees	Information Security Policy (EISP)
Acts of human error or failure	Social Engineering Awareness Policy (EISP)
Network Configuration Failure	Network Configuration Policy (SysSP)
Loss of confidential data	Data Breach Policy (ISSP)
Natural Disaster	Business Recovery Policy (EISP)

The above table lists all the threats that our organization could face and the corresponding policies describe how the employees are made aware of the threats and how the threats are handled using the various policies in the organization.

After determining the threat and the corresponding policy, we have also classified the policies into the various types of Information Security Policies.

For example, the Property of Intellectual Property Policy is classified as an EISP policy because this policy is applicable to all the regional offices globally. Similarly the Information security policy and Social Engineering Awareness Policy are classified as EISP and these policies ensure that all the employees in the organization need to have security awareness.

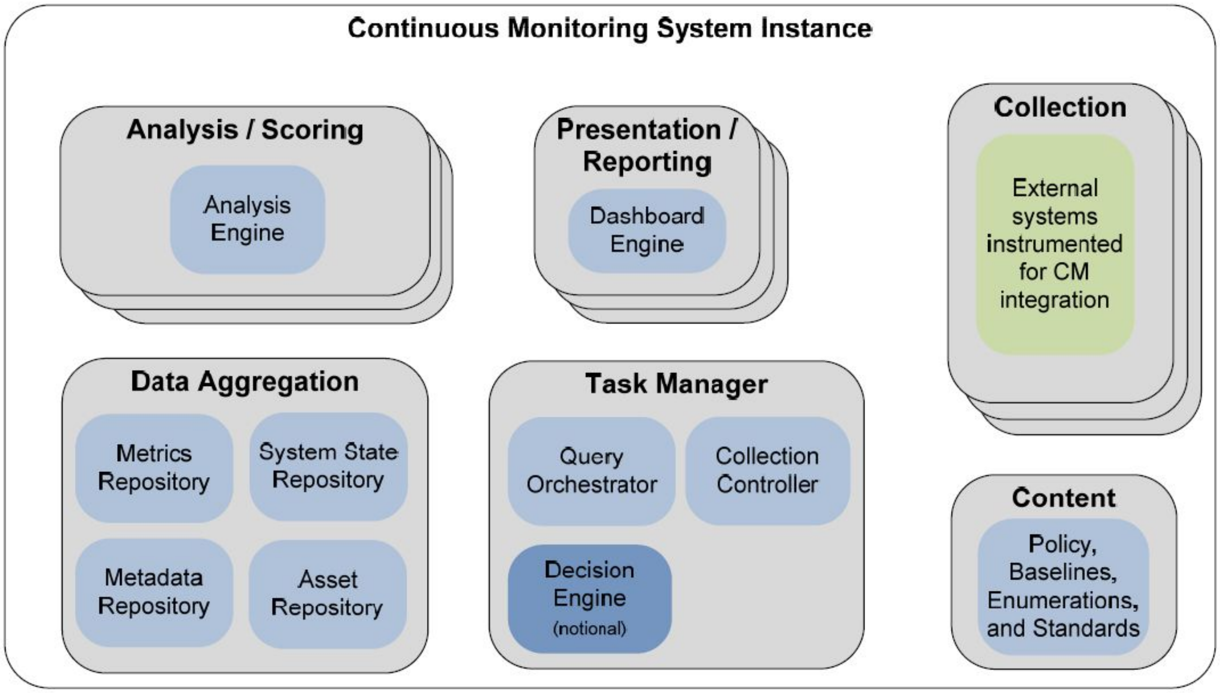
Security Monitoring

Continuous Monitoring

Continuous Monitoring is a very important part of security as it is the first step taken by the security engineers to understand how the adversary breached a network. In our organization, Continuous Monitoring is done with the help of the CAESARS framework (Continuous Asset Evaluation, Situational Awareness and Risk Scoring). The objective of this framework to provide awareness of threats and vulnerabilities to the various parts of the infrastructure.

Some of the external systems that could interface with the Continuous Monitoring framework are Vulnerability Management, Patch Management, Event Management, Incident Management, Malware Detection and Network Management.

Figure 7. Continuous Monitoring



The above figure shows the conceptual representation of the CAESARS framework in an organization. The Analysis/Scoring engine determines the possible risk of a security event in an organization. Presentation/Reporting processes the risk score and displays the same to the security admins. Collection works with the Intelligence reports from the external agents and integrates the intelligence with the SIEM system implemented in our organization.

SIEM (Software Information and Event Management)

The SIEM tools helps by working as a central repository for aggregating all the security events. It helps to add context and threat intelligence information to the security events to understand the baseline behavior. It also helps correlate data from the various security devices such as the firewalls, IDS and the IPS that could be integrated with our environment.

SIEM tools can profile the behavior of all the employees in our organization and this serves as a useful tool to understand the normal behavior of employees and the deviation from the normal behavior to understand the behavior of insider threats.

SIEM tools can assess the compliance posture of the organization and also separate the real events from non-impact events and locate and contain all the events.

ArcSight + Splunk

Splunk's motto – "Throw logs at me and I will provide a web based console to search through it intuitively"

ArcSight's motto – "We keep your business in business"

In our organization, Skyline we combine the capabilities of the SIEM tools – ArcSight and Splunk. It is important to understand the functionality of the SIEM tool before their implementation in our organization.

Splunk SIEM is best for the Log Management Layer it provides. The basis of Splunk is big data management where it helps us obtain a record from millions of records with a very simple query. Splunk can be integrated with all the security tools in the organization to collect logs including the Firewalls, IDS and IPS and also the Operating System logs.

ArcSight SIEM is best for the Correlation, Workflow and the Operational Management layer. These layers have been worked on in detail in ArcSight whereas Splunk was built mainly as log management tool which is very clear with the Splunk motto. The log management layer provided by ArcSight is not as sophisticated as the Log Management layer in Splunk.

Therefore, in Skyline, we integrate both the tools in our environment to understand the security events and respond to the events.

Cyber Kill Chain

The steps in the Cyber kill chain process is as below:

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation

5. Installation
6. Command and Control
7. Actions on Objectives

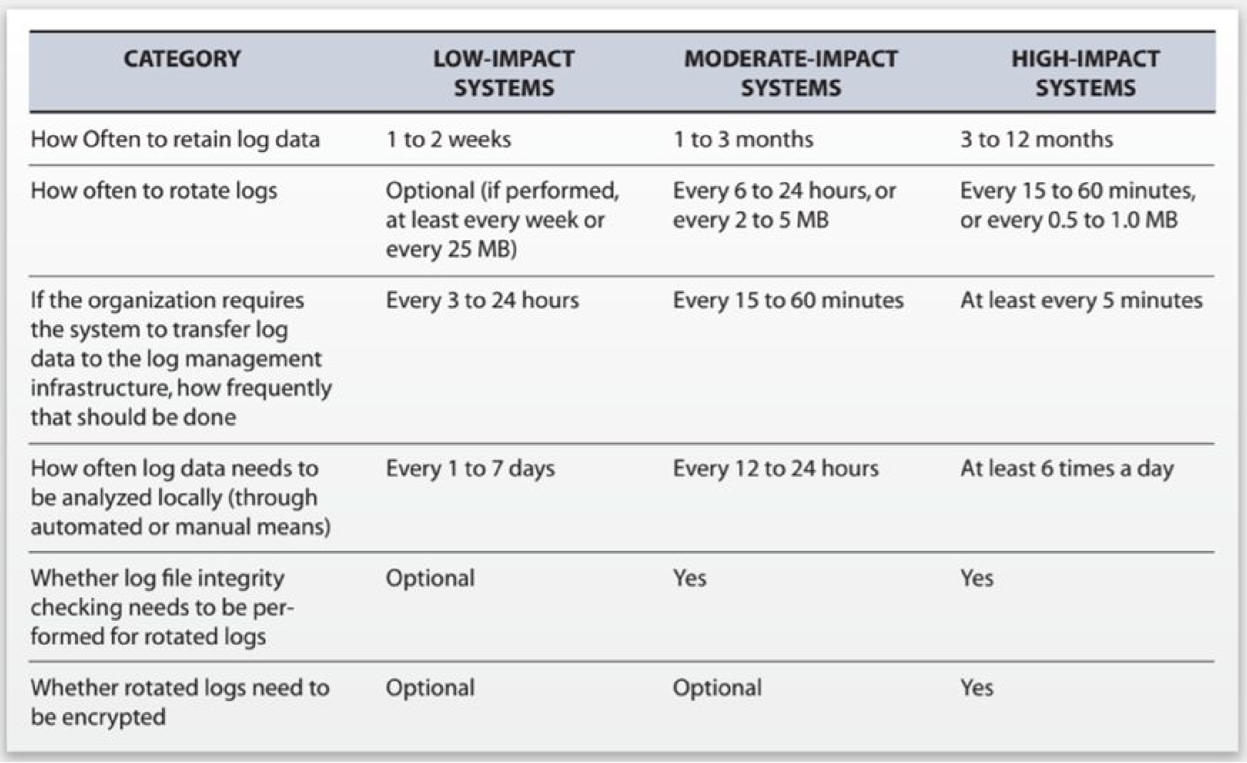
The attackers follow the cyber kill chain process to get into the network of an organization to steal confidential data such as client's information or Intellectual Property.

Trail of Attack is the information that is left by the attacker where it is a trail of the steps taken by the attacker to cause a security breach. Velocity of Response refers to the speed to respond to a security incident in an organization. Integrating Threat Intelligence information into the IDS, IPS and SIEM is very important.

The above graph shows the details about the various Intelligence Agents that were included into the organization protect the organization from attacks. The chances of the attacks reduces when the intelligence about the attacks in the organization is higher.

Frequency of Log Monitoring

Figure 8. Frequency of Log Monitoring



CATEGORY	LOW-IMPACT SYSTEMS	MODERATE-IMPACT SYSTEMS	HIGH-IMPACT SYSTEMS
How Often to retain log data	1 to 2 weeks	1 to 3 months	3 to 12 months
How often to rotate logs	Optional (if performed, at least every week or every 25 MB)	Every 6 to 24 hours, or every 2 to 5 MB	Every 15 to 60 minutes, or every 0.5 to 1.0 MB
If the organization requires the system to transfer log data to the log management infrastructure, how frequently that should be done	Every 3 to 24 hours	Every 15 to 60 minutes	At least every 5 minutes
How often log data needs to be analyzed locally (through automated or manual means)	Every 1 to 7 days	Every 12 to 24 hours	At least 6 times a day
Whether log file integrity checking needs to be performed for rotated logs	Optional	Yes	Yes
Whether rotated logs need to be encrypted	Optional	Optional	Yes

The above figure provides the details about the Log Monitoring process we are following in Skyline for the different types of the system such as Low Impact, Moderate Impact and High Impact.

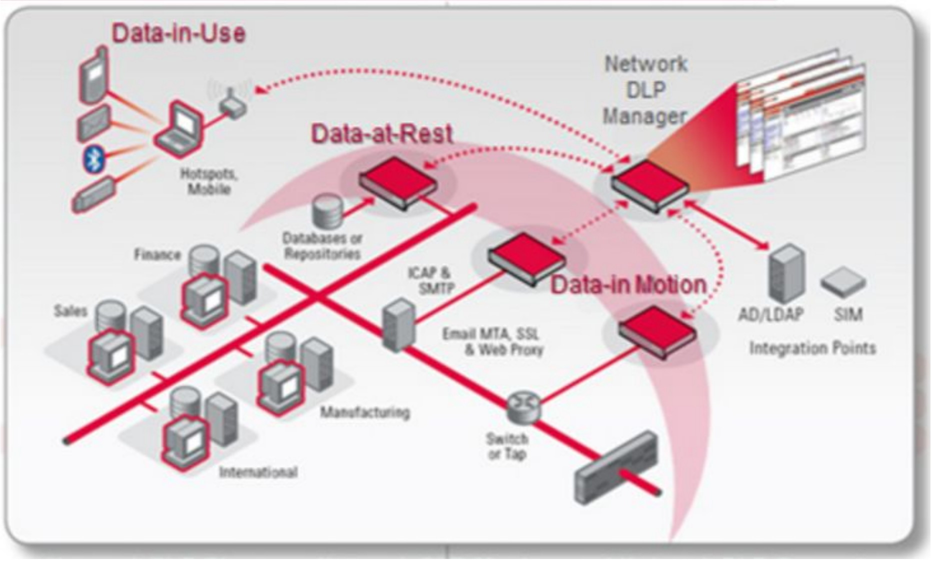
Behavioral Analytics for Insider Threats

Using SIEM tools we need to understand the normal behavior of employees in a particular department. If multiple employees who have the same access behave in the same manner by viewing similar types of files then it can be classified as normal behavior. An employee among a group of employees who does not behave in the same pattern and is known to view files he/she is not authorized to then that employee is showing traits of becoming an insider threat. Scope of the access provided to an employee plays a very important role in determining the insider threat.

Data Loss Prevention

Skyline uses the DLP process for tagging the important data by ensuring that the sensitive data is not lost. For this process, we are going to use the DLP tools from McAfee and integrate the same with our SIEM to track the security events. Sensitive data in files can be watermarked using the DLP tools and this watermark is entered into the DLP server within our network and ensures that the tagged data does not leave the organization in any form such as emails or employees trying to upload the data into online forums.

Figure 9. McAfee DLP Process



The architecture of the McAfee DLP process integrated with Skyline is shown in the above figure.

Third Party Vendor (TPV) Monitoring

Third Party Vendor need

Skyline is a multinational company that has been expanding and has been increasing its client base tremendously. We outsource some of our services to third party suppliers to reduce the cost of our services and thus the price of our services. Incorporating third party suppliers in our supply chain helps us in meeting our growing demand. Using third party vendors also help in enhancing the customer experience, this can happen by having closer branches that can service clients, more advanced networks that can provide better connectivity for users. As a financial company we use third party suppliers to:

1- Provide mobile solutions
2- Process data
3- Collect payments
4- Application development
5- Service our customers
6- Research and development

Increasing Risks due to Third Party Vendors

Many companies rely heavily on third parties like material suppliers and vendors to help them meet both their contractual obligations and consumer demand. This reliance is not without its risks, though. The risks that we face are interruption of services, different cyber attacks, breaching regulation and legal violations. Another downside to using third party vendors is that if any breach or hack happens the company is the one blamed and that loses its reputation. Even though some if a mistake is happens, based on the regulatory body, the ownership of the risk has to remains with the financial institution and not with the third parties performing the actions. This makes the company liable for all the actions of the third party vendors.

Third party Vendor Agreements

Since we are liable to all the actions of our third party suppliers we have to have rigid agreements and contracts that define the relationship between third party vendors and Skyline. To be able to come with specific contract clauses we studied Skyline’s status quo. First we have to define our tolerance for risk, because most of our transactions involve handling critical information such as CCNs, SSNs and sensitive PII Skyline has a very low tolerance for risk. We also heavily rely on our reputation, if it is tarnished then our business will suffer. Next define what privileges third parties have. Another part of the contract is defining what data they have access to including data on paper and hard copies of data. Furthermore, we make sure that we do our due diligence prior to signing the contract and any data exchange. Another Important aspect that we study about potential third party vendors is employee behaviour and action patterns, this helps us know the extend of data exposure and security. Another vital check that we perform is IoT device checks, this helps us have a good idea of the overall use of IoT devices by a certain third party vendor. A thorough analysis of these IoT devices, their manufacturers and the data they can access gives us a clear idea of all the possible ways of our data exposure. All these factors can be included in a scoring matrix that helps with choosing the most suitable vendor and drafting the most comprehensive and inclusive contract. The table below show that outcome of a risk scoring matrix of three potential vendors.

Table 10. Risk Scoring Matrix

Risk Factors	Vendor 1	Vendor 1	Vendor 1
PII/Regulated Data Shared	5	3	2
IP/Company Secrets Shared	4	2	2
Special Privacy Data	3	3	1
Weak Jurisdiction	5	3	1
Financially Unstable	4	2	0
Technology Resilience	1	2	2
Other Factors	3	3	1
Risk Score	23(High)	18(Medium)	9(Low)
Risk Scores High(>=20) Medium (<20, >14) Low (<14)			

To reach the most beneficial agreement and ensure that Skyline gets its third parties to comply with its needs and the regulatory body's demand we analyze previous transactions of the third party that we are interested in hiring. We also perform additional due diligence with respect to third party vendors in high risk areas. Next we use forums and publications that help with setting the standard for compliance and what is expected from a third party vendor. After that we also check the third party's compliance track record with its previous contract. We also make sure that our policies are not static, every year the company should do a survey to know what the peer companies are doing in terms of updating their codes of conduct and follow suite. Finally is it important to note that sometimes companies that have had a problem in the past and then mitigated that risk and solved the problem as a result become of low-risk.

Third Party Vendor Monitoring

As mentioned above, the company is the one that is liable for any non-compliance to regulations and standards. This means even after running screenings and checks to make sure that the third party supplier is of low-risk it is still important that we monitor them during the time they are providing services for Skyline. The first thing we do in third party monitoring is to:

- link vendors to contracts and engagement facilities
- Perform vendor profiling
- Assign vendor managers
- Use metrics and performance indicators to assess performance
- Document products and services provided by each third party vendor
- Track facilities and activities provided by each third party vendor
- Perform onsite and offsite audits to get assurance on practices followed by the suppliers.

Defining and tracking relation between a specific service unit and a service provider offers powerful capabilities for ensuring contract compliance. The aggregation of vendor profile data including the amount of money and time spent, this will facilitate developing strategic plans that maximize the the company’s benefit from its relations with its third party vendors.

Using this information, third parties are categorized into tiers, then a tailored assessment is produced for each tier that reflects the criticality of said third party. The third party vendors in each tier are assigned a different risk assessment and are subject to tailored screenings and benchmark tests. This classification for each tiers is based on the type of information handled, the amount of money and the type of clients they deal with on the company’s behalf. This is done with an automated workflow tool.

The tools then link answers from the questionnaire to contracts and compliance clauses for each third party vendor involved in each tier to automatically identify areas of noncompliance. After this step is complete, assigned personnel assess the type of noncompliance, report it to management and then work with the third party to remediate/resolve the areas of noncompliance. The tools that are used are can also be viewed in real time this gives the company a clear idea of the compliance status of third parties that they deal with and how much the company's overall vendor risk exposure is. These tools also help the company in drawing a holistic third party profile that can help with:

- Identifying and monitoring potential risks
- Tracking compliance with related policies, controls and industry regulations
- Instilling third party accountability by monitoring access to company assets
- Monitor incidents and use this data to cut-off risky third parties with frequent incidents.

Challenges of Third Party Vendor Monitoring

Moving on from the framework to the operationalization of 3rd party risk management, companies deal with two characteristics in their supplier base:
1- Geographical diversification and increased language dispersion
2- Increased number of suppliers which consequentially leads to increased amount of data that the organization has to deal with.

Solving these challenges manually is very inefficient and unlikely for a long term solution, this is one of the reasons we are embracing technology. A good example of this is risk assessment, workflow tools allow organizations to send a wide variety of questionnaires these can be audit related, risk assessment related, financial and non-financial. The company, with the help of the technology of the workflow tool, targets a much larger supplier base then it used to be able to, in a shorter period of time and track their responses much more effectively. Since Skyline is a multinational company the responses are in different languages, the company uses language neutrality tools that leverage NLP and NAG technologies.

It is important to note that when the company runs vendor screenings of hundreds of thousands of suppliers, which is an essential part of supplier risk management, this might result in hundreds of thousands of alerts. A normal percentage of false alerts can reach up to 95%, this makes it challenging and very expensive to spot those false alerts manually. As a large company we are making use of analytics tools to deal with this problem. These examples make it clear that manual intervention is not the solution. digitization is the solution.

Identity and Access Management(IAM)

In Skyline, the security team already has a basic identity and access management program in place. In the developed information security program, we are going to develop the existing identity and access management program to take into account the expansion that Skyline went through and also determine areas of improvement for the different types of information security policies. To be able to most effectively tackle this problem and ensure the best results we take feedback from the employees

Employee Feedback

To be able to most effectively tackle this problem and ensure the best results we take feedback from the employees. Here is a sample of the feedback taken from them:

- “The security team assigned long passwords for my company accounts that I find very hard to remember”

- “It takes me forever to access some information because of the multiple authentication that is implemented. This slows me down and slows our workflow system. My manager always blames me and this makes me feel incompetent”
- “I don't know if I should say this but I still get access to data and processes to the JP Morgan project we did last year ”
- “I feel this it is my duty to let you know that I was able to sign in to my colleagues account, I am loyal to our company and want our system to be safe”
- “I had a client meeting with Amado from HKS sales, our client from Kenya, and he told me they were not able to access their data there”
- “I am very annoyed overtime I call the help desk, the line is busy. I am starting to feel they don't their job or avoiding my calls”
- “My machine is very slow and I think it is because I have data from last year”

IAM Objectives

After analyzing the employee feedback using surveys and employee interview we also looked at the NIST framework we came up with objectives that the new system has to comply with:

- **Adhere to regulations:** This is done by periodic audits to make sure the IAM structure reaches the minimum qualifications of HIPPA, PIC and NIST. But, we also make sure that we are always trying to better ourselves and not just aim for the bare minimum.
- **Ensure Data security:** This is done by making sure only authorized and authenticated users can get access. The developed IAM does this using:
- Secure passwords and password managers, these are used to access data and login to accounts safely.
- Biometrics, these are used to access buildings that have high clearance or secret and top secret data. This also helps with keep track of which employee accessed what data.
- Identification Cards, these are used to access all buildings and help with keeping track of the time and place the employees are in.
- Tokens, these help with secondary authentication of a user.
- **Reduce privilege elevation**: Based on the feedback we got, we can see that some users still get access to information that they shouldn't be able access, because their work finished on that project. This might lead to privilege elevation. We avoid this by update access permissions periodically. The other side of the same coin is also performing access revocations periodically and reviewing the access revocation list to make sure that all the old employees donate have access to the company's information and the client’s data. Another solution that is implemented is creating alternate account for users to perform privileged actions. This lessens the time that an employee has privileged access therefore decreases the probability of a mistake happening and gives less time to malicious employees to carry out any maleficent acts.

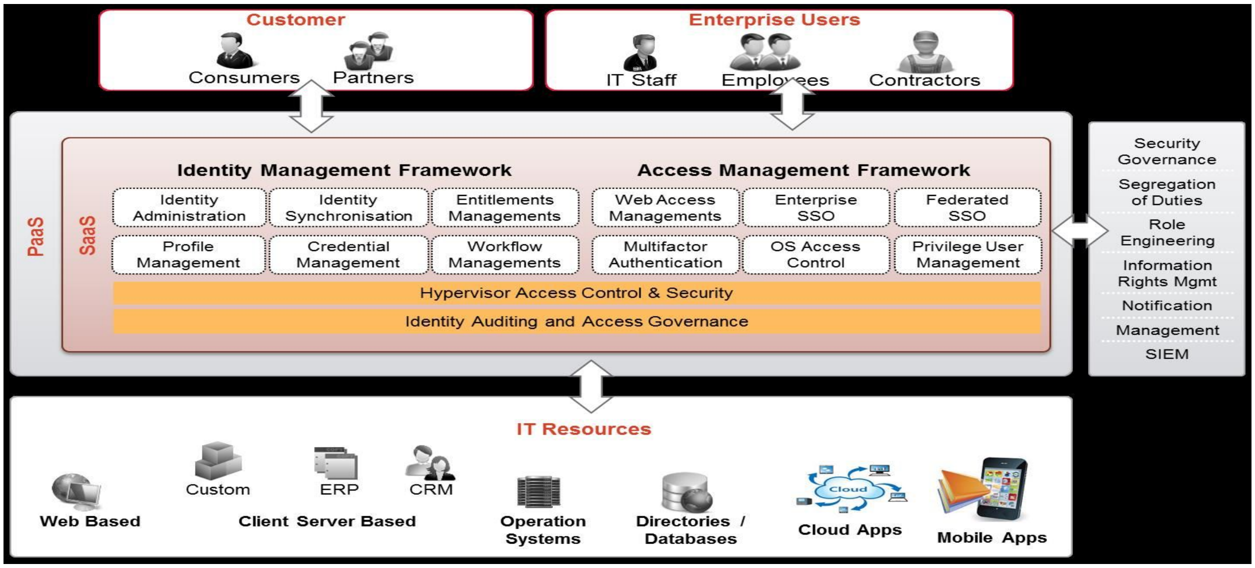
- **Fast, efficient and secure access for users**: This is done by reducing the number of passwords needed by each employee but making them more secure. It is also done by having password managers for some departments of the company. Another step that the IAM structure tries to do is exchange password for biometrics where it is feasible and more secure. Another aspect that is inline with accomplishing the goal of efficiency is automating help desk operations, this will allow employees to be self-dependent and eliminates the bottleneck at the help desk office.
- **Inline with business plan**: Security is very important for Skyline, but so is making profit. So to be in compliance with Skyline's business plan we use cost effective methods for IAM structure Ensure employees full potential is reached while maintaining the highest levels of security.

IAM Framework

The ultimate goal of the **IAM** Framework is '*to provide the right people with the right access at the right time'.* The IAM framework is divided into four parts:

- Authentication: This is done by a user providing sufficient credentials to gain initial access to an application system or a particular resource. IAM structure uses passwords, biometrics, ID cards and tokens to accomplish this.
- Authorization: In this area of the IAM framework the structure checks whether a user is permitted to access a particular resource. The IAM structure does this by comparing the access level and permission lists to the credentials of the employee requesting access.
- User Management: This area comprises of user management, password management, user and group role management. It defines the set of administrative functions such as identity creation, propagation, and maintenance of user identity and privileges. This area also manages the permissions and revocation lists and decides the level of clearance each users is granted.
- Central User Repository: This part of the IAM structure stores and delivers identity information to other services, and provides services to verify credentials submitted from clients.

Figure 10. IAM Framework



The figure above shows a general overview of an IAM structure. It consolidates all the different aspects of an IAM structure.

Additional IAM Features

After assessing the overall performance of the IAM structure we have decided to add some features that enhance the system's security and efficiency.

- **Monitor user resource access and sign in:** This feature monitors and reports any unusual and out of pattern resource access or sign in. This is done to enhance user accountability, the data that is collected is also used to track common mistakes and wrong practices and use it to tailor training programs to employees.
- **Implement Enforces access:** This feature helps with access time reduction and increases users efficiency, it uses a single password to access many applications. We at Skyline know the danger this might cause and thus limit this feature to certain employees who pass advanced security clearance.
- **Compartmentalization of data access:** This feature helps in lessening the effect of any unauthorized access.
- **Testing:** Testing the how the IAM structure interacts with the system is done using benchmarks and then reported using metrics.

Cloud Security

Skyline will implement a Hybrid Cloud service to support both public and private servers to fit the needs of the company's data. The hybrid cloud is able to offer flexibility and scalability. With the private cloud the company can store sensitive company data in the private cloud. The use of public cloud can range from traffic high traffic to testing/QA projects. Public cloud can store some of the companies less sensitive data such as emails.

NIST Publication 800-146 Cloud Computing Synopsis

The NIST Publication recommends several components for successful cloud security:

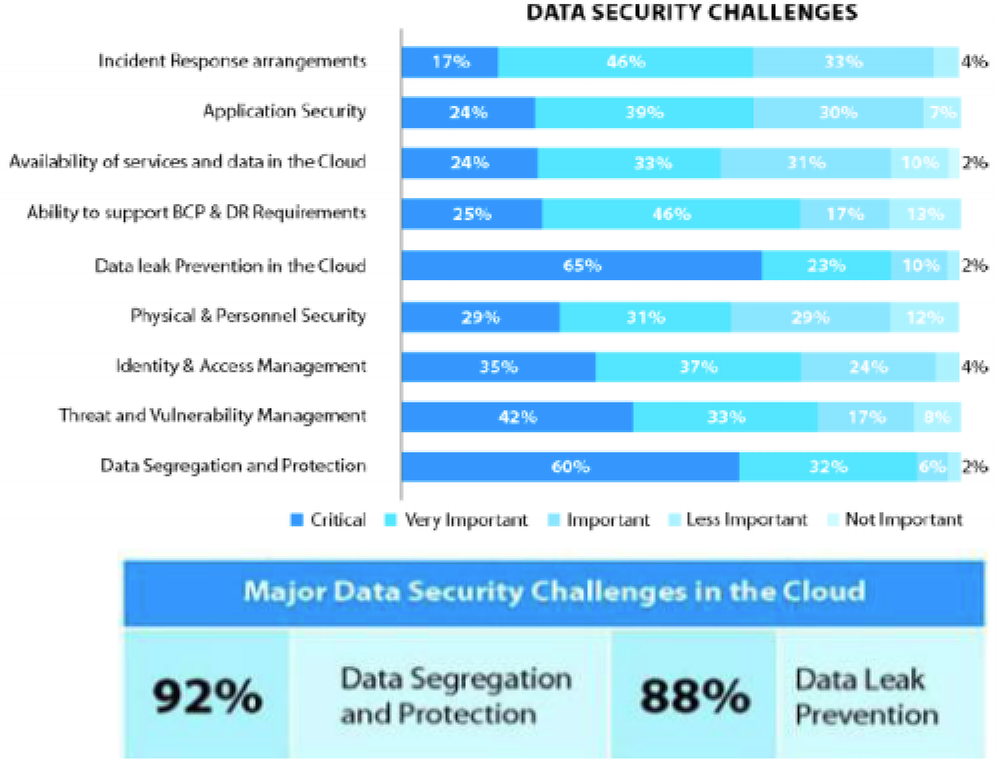
Table 11. NIST Cloud Security recommendation

Mangement	Migrating Data to and from Clouds Continuity of Operations Compliance Administrator Staff Legal Operating Policies Acceptable Use Policies Licensing

	Patch Management
Data Governance	Data Access Standards Data Separation Data Integrity Data Regulations Data Disposition Data Recovery
Security and Reliability	Consumer-Side Vulnerabilities Encryption Physical Authentication Identity and Access Management Performance Requirements Visibility
Virtual Machines	VM Vulnerabilities VM Migration
Software and Applications	Time-Critical Software Safety-Critical Software Application Development Tools Application Runtime Support Application Configuration Standard Programming Languages

Cloud Security Challenges

Figure 11. Data Security Challenges



Cloud Security Risk Mitigation

Public and private cloud data will be encrypted through the traffic as well as on the server. ISP failure mitigation will be in place by selecting backup ISP's. Because company downtime is unacceptable as a investment management firm there will be several Continuity Plan/Incident Response implemented.

Continuity Plan/Incident Response

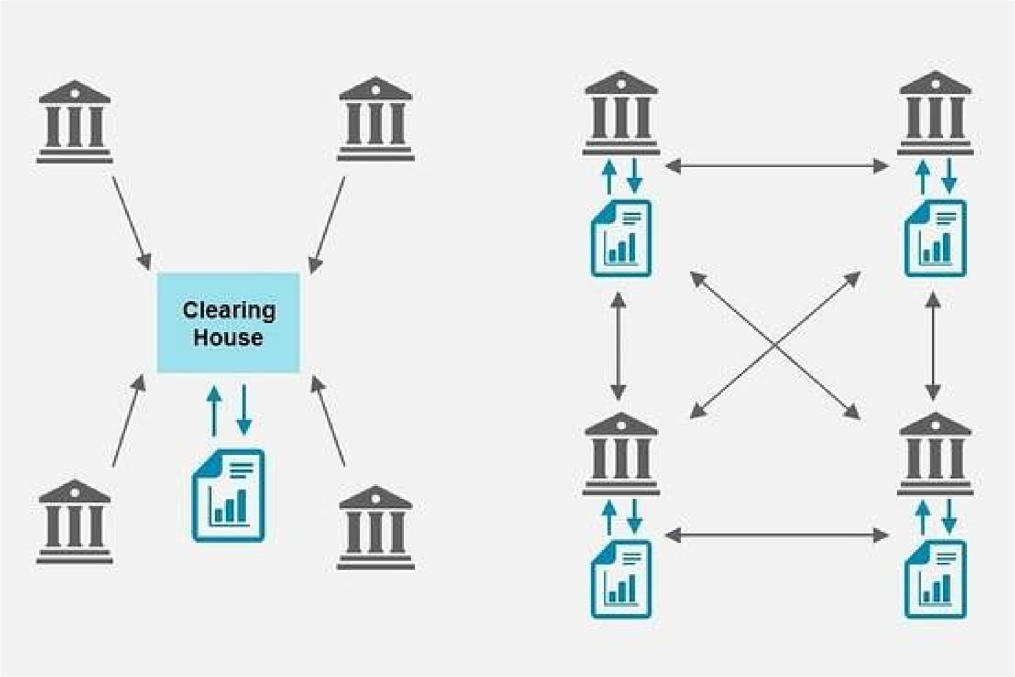
The company must establish the contractual agreements with the public cloud for responsibility in case of an incident. In case there is a problem on the public cloud's services, there must be an understanding on the overhead of their server architecture. For both the private and public cloud, frequent simulations of incident response must be run.

Blockchain or Cloud

As blockchain becomes more and more prominent in business, it may be a smart idea to invest the effort to incorporate it into our project queue. Major competitors like 'EY' are already taking steps towards development in blockchain technology. As cloud services took over the industry, blockchain technology may become the leading method for transaction processing.

This is because Blockchain successfully removes the middleman required for cloud and the opportunity for data corruption and theft.

Figure 12. Block Chain



For now it is a technology that may be too volatile and undeveloped for live implementation.

Mobile Device Security Strategy

This strategy covers approach to securing organization-provided as well as personally-owned (bring your own device, BYOD) devices. BYOD requirements are applied to all personally owned devices that have the ability to store, transfer or process any sensitive information from the Information Security Management System ("ISMS") scope. Such devices include laptops, smartphones, tablets, etc. The following key initiatives will be implemented to provide adequate security of Mobile Devices for complete protection of our information assets:

- Revise and update current **BYOD policy**
- Develop **System Threat Model** for mobile devices and resources that are accessed through them

- Implement **centralized mobile device management**. We are considering signing a contract with a third party vendor, which is capable of managing various brands of mobile devices as well as laptops.
- Follow five-phase **Mobile Device Solution Life Cycle** while incorporating Mobile Device Strategy

BYOD Policy

We will revise and update current BYOD policy, focusing on the following key aspects :

- ### Selective BYOD Approval

BYOD should only be approved on a case-by-case basis for those employees who require immediate and frequent contact with colleagues, clients or partners, regardless of their physical location or in situations when productivity gains outweigh possible risks and high cost.

- **Data Policy**

If a document contains any type of sensitive data, defined in Information Security Management System ("ISMS") scope, it is not allowed to be stored locally on personal devices. It is also not allowed to access our Trading, Reporting and Accounting systems from mobile devices or personally-owned laptops. In addition the company reserves a right to remotely or physically wipe all data from personal device at any time.

- **Mobile Device Management (MDM) Policy**

The company provisions installation of encryption technologies, security certificates, antiviruses, local firewalls. Every device entering Skyline's network must comply with password, screensaver and encryption requirements. Certain applications will be removed or blocked from a device. Security scans will take place daily

- **Loss and Theft Policy**

Any lost or damaged device must be immediately reported to Information Security personnel, so any data existing on it can be remotely wiped, security certificates destroyed.

- **Employee Termination Policy**

In the event of employment termination, employee is required to turn in any device, that was at any time registered on Skyline's network for examination and removal of any corporate data and access to business applications.

Mobile Device Threats

Our BYOD policy prohibits storage of any sensitive data locally on mobile devices or personally-owned laptops. Thus in case of loss or theft, malware infection or mobile browser hacking, the primary assets at risk would be user's credentials, user's personal data (or work notes which could be confidential), email communication (IMAP downloaded messages). In some cases of malware and hacking mobile device can be used as communication interception tool.

Table 12. Mobile Device Threats

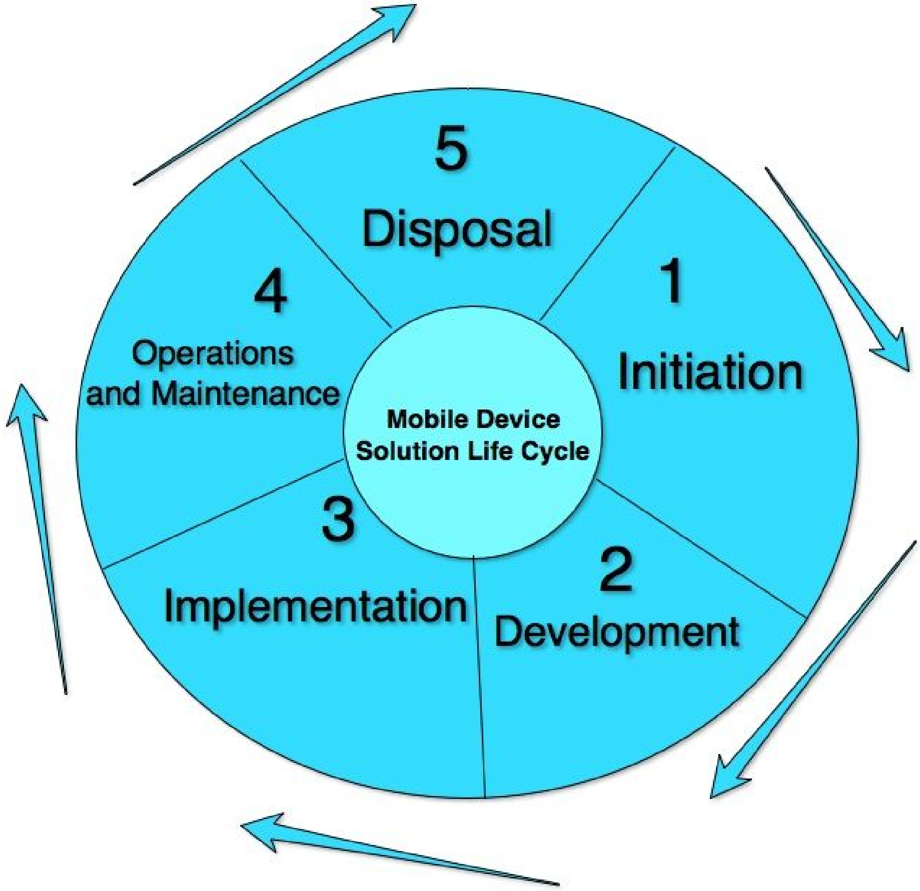
Threat	Asset at Risk
Physical Access (theft)	User's credentials, User's data, email communication, network access
Malware	User's credentials, User's data, email communication, network access
Mobile Web Browser Hacking	User's credentials, User's data, email communication, network access
Communication Interception	Corporate and personal information

Life Cycle of Mobile Device Security Strategy

While implementing our Mobile Device Security strategy we will follow five-phase Life Cycle, based on guidelines provided by NIST Framework [2]. The five steps are as follows:

- Initiation - Preliminary work, including identifying business needs, business vision on how mobile devices support company's mission, developing BYOD policy
- Development - Defining technical specifications, including authentication methods, encryption mechanisms, types of prohibited mobile devices models (we do not plan to work with Huawei and several Samsung models). Central Mobile Device management vendor is selected at this stage
- Implementation - Few devices are selected for piloting new mobile device management strategy. After extensive testing the systems are being implemented in production
- Operations and Maintenance - Security-related tasks, including patching, log monitoring and attack detection
- Disposal - Retiring mobile solution system or its components, safe equipment disposal

Figure 13. Mobile Device Solution Life Cycle



List of References

1. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf
2. http://www.eci.com/blog/439-developing-a-byod-policy-for-your-hedge-fund.html
3. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf
4. http://www.sciencedirect.com/science/article/pii/S1877050915006808
5. Whitman, Michael E., and Herbert J. Mattord. *Management of Information Security*. Vol. 4. Boston, MA: Thomson Course Technology, 2004. Print.
6. http://www.businessinsider.com/the-importance-of-business-process-maturity-in-running-a-hedge-fund-2011-9
7. https://www.sans.org/security-resources/policies
8. http://csrc.nist.gov/publications/drafts/nistir-7756/Draft-NISTIR-7756_second-public-draft.pdf
9. https://www.sans.org/reading-room/whitepapers/analyst/continuous-monitoring-is-needed-35030
10. http://infosecnirvana.com/splunk-enterprise-need-know/
11. https://www.sans.org/reading-room/whitepapers/analyst/killing-advanced-threats-tracks-int

elligent-approach-attack-prevention-35302

12. http://csrc.nist.gov/publications/PubsSPs.html#SP-800-150
13. https://en.wikipedia.org/wiki/Cybersecurity_Information_Sharing_Act
14. https://www.kingcounty.gov/operations/it/about/strategy/~/media/operations/it/governance/policies/Enterprise_Information_Security_Policy_signed.ashx
15. http://www.computerweekly.com/tip/Data-backup-and-recovery-software-A-financial-services-case-study
16. https://www.youtube.com/watch?v=3wlIx8BnLQs
17. https://www.youtube.com/watch?v=jz1wEWofo-I
18. http://ithandbook.ffiec.gov/media/22151/ex_nist_sp_800_34.pdf
19. http://www.eci.com/blog/439-developing-a-byod-policy-for-your-hedge-fund.html
20. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf
21. http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf
22. https://en.wikipedia.org/wiki/Blockchain_(database)
23. http://www.techmahindra.com/services/infrastructure_management_services/offerings/security/offerings/identity_access_management.aspx
24. https://www.youtube.com/watch?v=FD4soiaPWm4:
25. https://www.youtube.com/watch?v=7Oi5J8QRhxw:
26. https://www.youtube.com/watch?v=dtaRf2Fx_2U:
27. http://pwc.to/16JJjME