Marvel Studios - Secure Image Solution (MS-SIS)

Project Team

Aviraj Ajgekar (aa4691)
Shikshya Bhattachan (sb5925)
Abhishek Balaji Venkataraaman Sangeetha (avs395)

Table of Contents

Revision history

Version	Date	Author(s)	Notes
0.1	3/21/2017	Aviraj Ajgekar	Prepared the first draft for the preliminary gate review
0.2	3/29/2017	Shikshya Bhattachan	Added Guiding Principles
0.3	4/10/2017	Abhishek Balaji Venkataraaman Sangeetha	Updated Information Security Risks
0.4	4/15/2017	Shikshya Bhattachan	Updated Goals
0.5	4/25/2017	Abhishek Balaji Venkataraaman Sangeetha	Added Governance
0.6	5/1/2017	Aviraj Ajgekar	Added Management Section
0.7	5/5/2017	Shikshya Bhattachan	Added Assurance
0.8	5/8/2017	Abhishek Balaji Venkataraaman Sangeetha	Added Legal for MS-SIS
0.9	5/10/2017	Shikshya Bhattachan	Designed and updated BCDR (Business Continuity & Disaster Recovery) Plans
1.0	5/13/2017	Aviraj Ajgekar	Merged Strategy & Roadmap for MS-SIS in the final version

Introduction

Marvel Studios - Secure Image Solution (MS-SIS)

Marvel Studios Information Technology (MSIT) is reaching out the InfoSec team work build this project document about designing the information system security and engineering guidelines for **Marvel Studios - Secure Image Solution (MS-SIS).** MS-SIS is an Marvel Studios internal Line-of-Business (LOB) application that is primary used for handling and processing critical business data for MS employees.

This project document shall create a common understanding within the MSIT project team for Marvel Studios as well as between the project teams within the organization along with InfoSec Teams and Project Executive Sponsor.

Purpose

The purpose of this project document is to define and understand view on information security from a broad systems perspective at the same time view information security from a management perspective (government or corporate) perspective. In this project, we will study how to design a solid information security design plan by integrating Security into a Systems Engineering Process.

This project includes defining the vision, the mission and the services to be provided as well as the organization that will provide these services and the governance processes to manage this entity.

Audience

The intended audience for this project are critical Marvel Studios IT applications or systems. Information Security Teams (ISM) from Marvel Studios IT (MSIT) Security will work with respective business processing units to identify the critical applications and help onboard. MS-SIS is one of the applications that will be covered in this document.

Intended Audience by roles

MSIT Standard Owners;
MSIT Cloud Application Owners;
MSIT Engineering Heads;
MSIT Engineers

Scope

1. MS-SIS Mission Needs Statement

The Marvel Studios (MS) is commercial fashion photography studio working in the New York City's fashion district. The Marvel Corp (MS) is responsible dealing with high profile models in the Manhattan and outside boroughs. The company schedules many modeling assignments around the city. MS however on weekly basis generates a lot of images and data such as contractual agreements and billing invoices. To store the large amount images and contract papers MS is looking for a solution. However, being the non-IT company MS would like to leverage a cloud computing based solution to simplify their IT needs.

MS needs a secure cloud based solution to store the pictures/images and scanned contract document encrypted so that any unauthorized accidental leaks/breaches should not impact company's brand image as well as protecting celebrity portfolios being attacked. The proposed **MS-SIS** solution will be a local thick client application that MS will install on all systems. It will allow its photographers to upload images using their unique identity with an encrypted connection to the cloud based storage with a unique encryption key and authentication mechanism where each photographer can only upload and access its own set of pictures/images.

2. Scope of the system and security engineering analysis task.

In this task, we will document the functional requirements, operational environment, system boundaries and logical interfaces, and user classes for the **MS-SIS** system. Based on this information, we will perform a system security engineering study to include:

1. Risk Analysis
2. Security Requirements (Multi-Factor, Encryption, KMS)
3. Technical and procedural architectures and methods to satisfy these requirements (countermeasures)
4. Policy considerations, including impact on security requirements and countermeasures (Key Rotation)
5. Identification and analysis of legal issues that may impact security requirements and countermeasures (Compliance, Legal)
6. Planning for the security management of the deployed **MS-SIS** system, including management of all countermeasures, monitoring for new threats, and ensuring that all IT management processes support the goals of security (Machine Learning and Threat Detection)
7. Contingency planning for security breaches
8. Auditing, Alerting and Reporting mechanism

3. User Classes, System Boundaries/interfaces, and Operational Environment

The following are assumed for the **MS-SIS** system:

3.1 Operational Environment: MS-SIS will be deployed into public cloud environment and there will be a client software package installed on local systems like desktops and laptops. All network connections to the **MS-SIS** servers will be over the secured TLS/HTTPS based public internet connection.

3.2 User Classes:

1. External clients (models and celebrities), who want to access their profiles pictures/portfolios using public website.
2. MS Photographers (internal users), who are responsible for encrypting and uploading the pictures/images to the cloud based solution.
3. MS Cloud and Security Administrators (internal users), who are responsible for all aspects of managing cloud based system operations including building an identity and key management solution.
4. MS Application Managers (internal users), responsible updating, patching and uploading the new version of the proposed solution including periodic back-up of the data.

3.3 System Boundaries: The **MS-SIS** system includes all **MS-SIS** servers, the MS Cloud and Security Administrators, and the **MS-SIS** Application Managers. Note that insiders are considered part of the system.

3.4 Interfaces:

External Clients: Interface is through a web browser on a client machine. The **MS-SIS** solution website is accessible over the public internet.

MS Photographers (Internal Users): Interface to **MS-SIS** includes both web browser and cloud portal based backend access. Connectivity is the TLS/HTTPS based public internet connection.

MS Cloud and Security Administrators: Interface to **MS-SIS** includes both web browser and cloud portal based backend access. Connectivity is the TLS/HTTPS based public internet connection.

MS Application Managers (internal users): Interface to **MS-SIS** includes both web browser and cloud portal based backend access. Connectivity is the TLS/HTTPS based public internet connection.

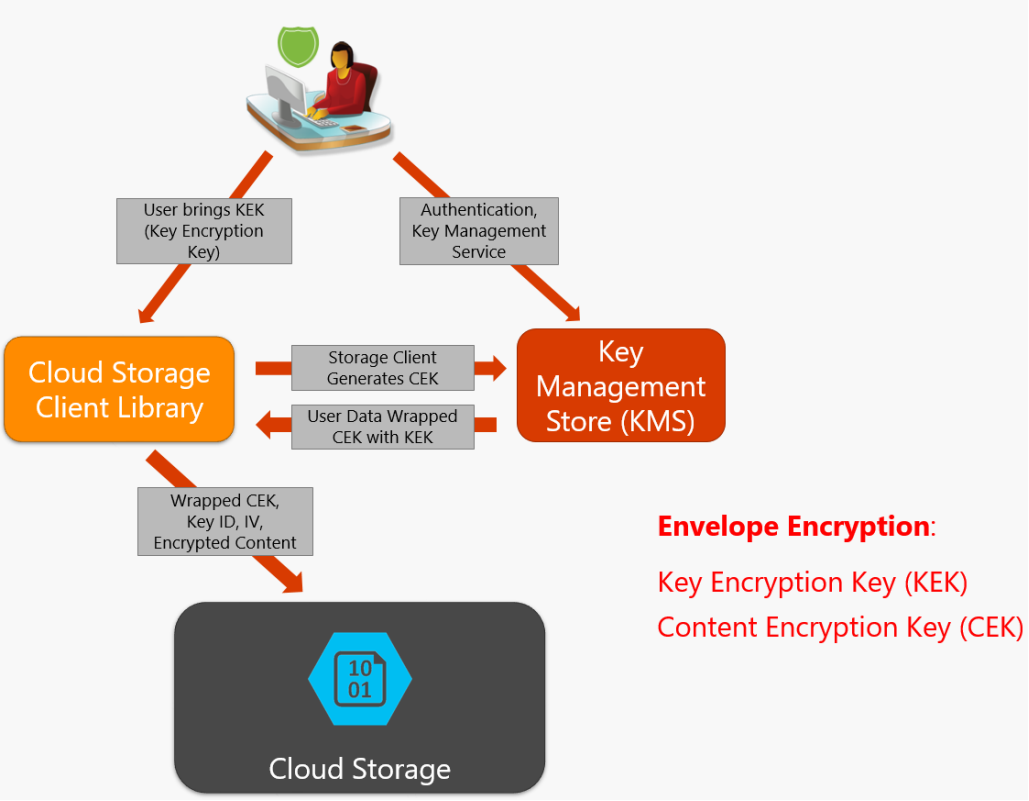
4. Use Cases and Functional Flow Diagram

The basic Use Case covers the scenario where a MS Photographer has pictures ready to be uploaded to the cloud based solution using its unique identity and encryption key that will be stored into the cloud based key management service.

This use case can be outlined as follows:

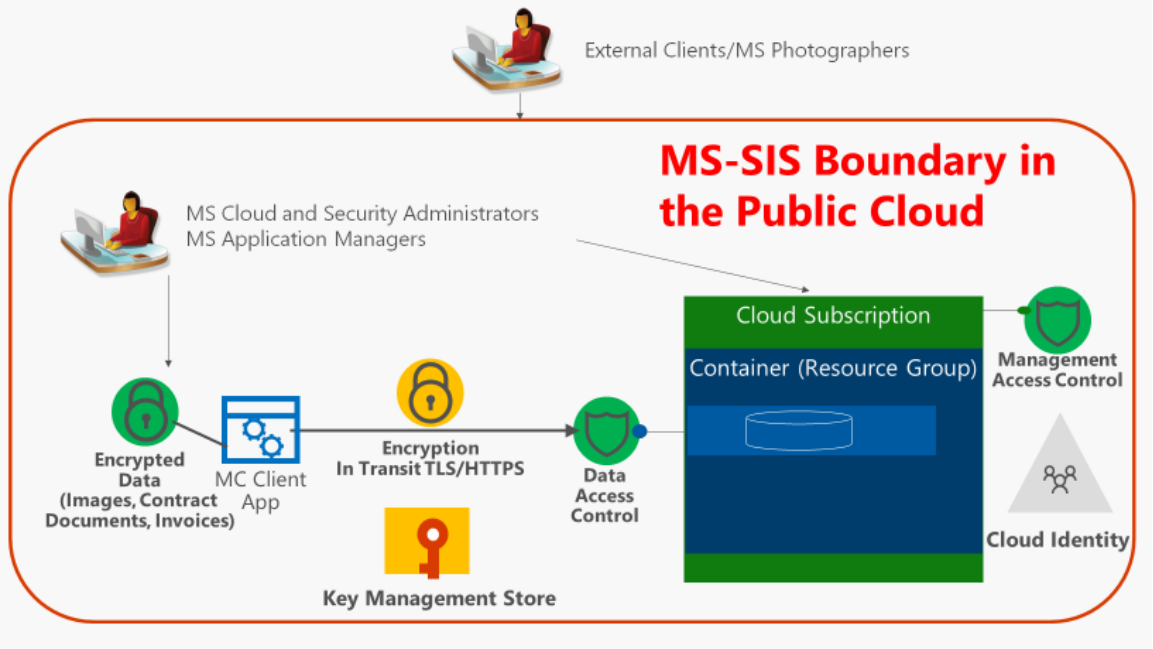
1. MS Photographer brings Key Encryption Key (KEK) to key management service store
2. Cloud Storage Client Library generates a Content Encryption Key (CEK) for pictures/images
3. The pictures/images are then encrypted using CEK
4. This CEK is wrapped using Key Encryption Key (KEK) – Additional Wrapper…
5. MS Application Managers have already specified Key wrapping method
6. Cloud Storage Client Library never has access to the KEK
7. Lastly, the encrypted data along with wrapped CEK is stored as the pictures/images metadata on the encrypted pictures/images (BLOB Objects)

The **functional flow diagram** (i. e., the diagram that shows the flow of information for this function) for this use case is shown below.



Additional use case/functions will be defined in the execution of this project to describe the activities of the internal users (MS Cloud and Security Administrators, MS Application Managers).

5. System Boundary diagram



6. Key Security Issues

The key security issues we expect to deal with for **MS-SIS** are:

1. Protection of models/celebrity photographs (Pictures/Images), Contractual and Billing Invoices documents using Encryption/Key Management Store.
2. Secure connectivity to the cloud based solution from client machine for external and internal users.
3. End to End Encryption in Transit and Data Access Control during upload and download of the data for the external as well as internal clients.
4. Role-Based Access Control (RBAC) model for internal users so that they can perform only specific tasks within the **MS-SIS** boundary, when performing update, patches, backup etc.

Other security issues may come up in the risk analysis and will also be dealt with.

Executive Summary

We, at Marvel Studios (MS) already trying to explore new opportunities for our organization and to deliver the best experience for our customers. Marvel Studios is one the top studios in the commercial fashion photography industry based in the heart of New York City's fashion district. The Marvel Studios (MS) is responsible dealing with high profile models in the Manhattan and outside boroughs. The company schedules many modeling assignments around the city. Even though MS is not a technology company, we are already equipped with cutting edge technologies and equipment when it comes delivering our core business for our customers. That includes using state-of-the-art camera equipment or leveraging commercial grade studio software. Marvel Studio (MS) is always open to try and explore modern technologies to deliver the best class results. In this digital era where every organization is going through Digital Transformation, Marvel Studio (MS) is destined to breakthrough to take new challenges. Thus, even being the non-IT company Marvel Studio (MS) would like to try new modern infrastructure and application solutions for their upcoming project dubbed Marvel Studio – Secure Image Solution (MS-SIS), a hybrid cloud computing based solution to simplify the overall business experience for Marvel Studio (MS).

In order undergo digital transformation, Marvel Studio (MS) has been evaluating various options for their upcoming project MS-SIS. We, at Marvel Studio (MS) realized that in order to transform we have to look at next generation solution and transform ourselves to stay ahead of the competition. Therefore, Marvel Studio IT (MSIT) decided to look into public cloud based solution with a security in mind to store the pictures/images and scanned contract document encrypted. Marvel Studio (MSIT) teams have been evaluating the cloud options for quite some time and at this stage we are ready plan the next stage for this MS-SIS Project. We have been hearing a lot about various attacks and breaches every other day. Therefore, in order to deal with any unauthorized accidental leaks/breaches and not impacting company's brand image we are building this project report to study and understand risk, threats, various policies and thus building a strong security design. This project document will become a solid foundation for our digital transformation journey for next 12-36 months of roadmap.

The proposed MS-SIS solution will be a set example of what's the Marvel Studio (MS) vision is all about, we will be making sure to incorporate all the new technologies such as Blockchain, Hybrid Cloud technologies, next generation credentials and various other cloud computing and agile methodologies to deliver a secure cloud based solution. At the same, the solution that will be secure enough to take care of any internal and external threat. Technologies such as machine learning, big data analytics will help us track and deal with any known and unknown threats.

Lastly, as a part of our digital transformation we are committed to continuously investing into our information security and engineering strategy to make sure that we are continuously exploring new technologies, new threats and become ready to embrace digital transformation.

Current state

This is current state

Business Direction

This section will provide a high-level view of evolving business and technology strategies and the impact on information security.

Marvel Studios (MS) is going through digital transformation that means we are transforming both in terms of business strategies as well as in terms of our technology strategies in the coming months. Marvel Studios (MS) has always been a closed group in terms of technology that means we have not explored much of the public cloud offerings and at the same time our business model focused in the New York City based environment.

Now that Marvel Studios (MS) is expanding and we are looking through the new opportunities through our digital transformation, this is a great opportunity for us to re-evaluate our business and technology strategy by spending time with our executives and leadership teams. In the past few months, there have been a strong message around the organization that we have a company have to transform and we are taking bold steps to define new business strategies that means using new collaboration ways, leveraging mobility as one of the ways to deliver great results.

Marvel Studios IT (MSIT) group is also excited about this change, we have been working with Marvel Studios (MS) IT team to help build the strategy and vision for Marvel Studios (MS) as what we could accomplish in the next 12-24 months from technology perspective. What are the emerging trends and technologies available for us. How can we embrace those technologies in a secure way without interrupting our business or causing any impact to our data? Marvel Studio IT (MSIT) will be working with different InfoSec groups to assess the gaps between the technology and the security areas, document them and will keep us updated in our continuous dialog on what all is changing and how can be effectively lead with the technology landscape in the coming months.

Critical Information Assets

This section will provide a high-level view of the information that is critical to the business.

Marvel Studios – Secure Image Solution (MS-SIS) will be dealing with the "risk assessment and analysis" In this context "risk" will be referred in terms of information security. Risk analysis is a process of systematically identifying the assets, threats and potential vulnerabilities.

For Marvel Studios – Secure Image Solution (MS-SIS) about assets at risks we are talking in terms of IT assets. Any asset at risk will be mapped back to the MS-SIS IT asset at risk. When we say assets at Risk we mean Infrastructure, endpoints, software applications, financial data, credit card data, PII Data, Process that run on IT system etc. Additionally, that include "process" or "function" related asses too. However, information is usually the primary asset.

For MS-SIS, IT Assets at Risk can be broadly categorized in 3 categories.

- MS-SIS Information Assets - **Pictures / Videos / Contracts / Intellectual Property**
  - MS-SIS Celebrity Pictures, Photos
  - MS-SIS Videos (HD, 4K)
  - MS-SIS Data Processing Algorithms (Filters, Custom Rendering etc.)
  - MS-SIS unused RAW Footage (Audio, Video, Images – Pictures/Photos)
  - MS-SIS Studios Software Licenses, Agreements
  - MS-SIS 3rd Party Vendor Equipment Inventory and Database

- MS-SIS Business Processes – **Compliance Regulatory and/or Financial/Intellectual Property**
  - MS-SIS Studio related patents
  - MS-SIS Data Access related Process/Approvals
  - MS-SIS Contract Papers, Agreements with Clients
  - Financial Reports, Data
  - MS-SIS Data Distribution Process
  - MSIT Processes for handling and transferring data

- MS-SIS Infrastructure (Studio, IT Equipment, Cloud, Servers, Drives etc.) - **Operational**
  - Marvel Studios (MS) - Camera Equipment (SLR, DSLR, Film Cameras)
  - Marvel Studios (MS) Video Recording Equipment
  - Local Infrastructure like Laptops, Desktops, Digital Printers, Scanners
  - Storage Arrays – SAN, NAS, File Shares
  - Public Cloud Based Infrastructure
  - Local Networking Links, connectivity to Internet and Cloud

These are some of the broad categories of the assets at risk that we have covered for our MS-SIS.

Threats

This section will provide a view of the security threats that drive the greatest risk to the company's critical information assets.

MS-SIS solution is cloud based solution. That means there will be a public connectivity. At the same time a lot of information is stored locally within the Marvel Studios (MS) on-premises infrastructure. Therefore, given the hybrid nature of the solution we have to understand and categorize different types of threat agents that could be impacting MS-SIS. From our class slides, a threat is a "threat agent" that wants to compromise the asset with some specific goal in mind (the person and the goal)

Threat Agents with classification for MS-SIS Solution

- MS-SIS Classified Information: Threats from other studio organizations within United States.

- MS-SIS Financial Assets (Financial Information, Compliance/Regulatory Data) – Threat agents include insider employees or foreign hackers, outside systems)

- MS-SIS Intellectual Property (MS-SIS Data Processing Algorithms, Data Storage and Management Process, Custom Rendering Process): Threats from people who can use the information from competitors, or potential customers (Other Cinema Studios competitors or rival corporations seeking a competitive advantage)

- Marvel Studios (MS) Computing/Networking Resources (IT Infrastructure and Cloud Infrastructure): Threats from people from outside hackers, criminals)

As you can see that there are different forms of the threat agents, and they are all over around use.

And the finally the **INSIDERS…with ACCESS** within the MS-SIS Environment.

The **Insiders** are either great threat agents or being used the outside threat agents using "social engineering" for e.g. a MS-SIS Vendors could be in relationship with someone outside who might be using contractor's credentials to access company information or trade secrets.

"**Anything**" connected to the MS-SIS network internally is vulnerable and since the insider can be accessing network there might be a possibility of an attack or perform some tasks like releasing virus or something else.

Insider MS-SIS employees are not different class of threat agents but the example of the other classes of threat agents with better access to the system.

Some of the motives/objectives of the threat agent.

At times the threat agents do the things for various reasons and different motive, there is no fixed set of reasons for MS-SIS SYSTEMS.

- Theft for cause financial impact to the company.
- Theft for stealing MS-SIS Intellectual Property like algorithms, patents, rendering processes, data distribution process etc.
- Extortion based threat on threat of information disclosure like celebrity data leak. (reputation damage)
- Theft of information for commercial purpose (Competition with a different Cinema Studios)

Information security gaps

Assess gaps for each security functional area

Marvel Studios IT Organization is always making sure that we are using the state of the art security technologies that we could let our employees to their jobs with the utmost productivity. While we are building this solution for our employees as well as the people on the field like photographers, editors, mixing teams etc. we still feel that there are still lot of things from the security and governance perspective are needed.

Take a simple example when we have so many people working on a celebrity portfolio, we generate a huge amount of content and then it becomes a responsibility of the firm to rightfully take care of all the copyright material. Think about a scenario if there is a data leakage. It may be a couple of images for a celebrity, but it could go a long way hurting Marvel's Brand.

Some of the most crucial security gaps Marvel IT could foresee are as follows.

- DLP (Data Leakage Prevention) Tools and Technologies
- Information Rights Management
- Consistent Data Backup Solution
- End-to-End Security Response Team in case of any incident
- Integration of the next-generation technologies like Machine Learning, Security Detection Mechanism
- Predictive Analytics for the IT Security

These are some of the security that Marvel Studios IT would like to fix in the coming months.

Information Security Risks

This section is a summary of business activities that are not being performed in a secure manner and the risks they create.

To do a complete Information Security risk analysis, the first step is to find out the vulnerable areas in the system which mainly include the process of storing and retrieving information securely.

Risk Management:

The important part of risk management is to find and prioritize risks. When this is done, it becomes easy to identify the most critical risks which makes it easy to manage or mitigate them. By prioritizing the critical risks and managing them first, there is a high chance that the less critical ones get mitigated automatically. We keep track of which risks are managed as each solution is discussed and this makes managing the other risks easier. There are multiple steps in risk management which are discussed as follows:

Risk Analysis:

Impact:

In this step, we measure the impact of a threat on an asset. There are various methods that can be used to measure the impact of a threat, for the MS-SIS we are using a Qualitative scale which will be discussed later. This impact scale was designed to prioritize the risks based on the impact to the organization. The impact scale used for the Secure Image Solution is a four-category scale

Scale	Impact
Low	This scale is used to define low level threats that affect the organization on a small scale. Since we are using a public cloud service to store data there are risks surrounding this which will not cause a direct impact on Marvel Studios. Additionally, this impact scale is also used to categorize financial and regulatory compliance which may cause small issues that may occur infrequently.
Moderate	This scale is used to define risks that affect the organization on a moderate scale. This scale is for threats that have a possibility of happening more than the Low scale. Additionally, this impact scale also

	categorizes threats that may happen day to day and not cause any major problems in the workflow but could cause serious problems if not treated eventually.
High	This scale is used to define risks that may have a severe impact on Marvel Studios , organizational operations, assets and individuals involved , the threat event that fall in this category may (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm/loss to individuals .
Critical	This category is used to define risks that may cause multiple severe or catastrophic impacts on Marvel Studios

Now to understand how the impact scale is formed we define what kind of losses each scale represents

	Low	**Moderate**	**High**	**Critical**
Loss (monetary)	<1k	1k-100k	100k-10M	>10M
Legal	Fine	Small claims court	Individual Law suits	Class Action Law suit
Safety	None	Minor Injury	Hospitalization Required	Permanent damage / death
Safety (Assets/ Operations)	Minor bugs		System crashes	Total System failure

Likelihood:

The impact of a threat on the organization is paired with likelihood to prioritize the risks. Likelihood is an indication of the probability that a potential vulnerability may be exercised given the threat environment. We Consider the following factors:

1) Threat-source motivation and capability

2) Nature of the vulnerability

3) Existence and effectiveness of current or planned controls

Scale	Likelihood
Low	The event is not very likely to occur; i.e., once or twice a year
Moderate	The event is somewhat likely to occur; i.e., 1-10 times
High	The event is most likely to occur
Critical	The event is almost certain to occur

Impact by critical IT asset :

Now that the scale for likelihood has been defined we now see how the loss of the IT assets associated with the system are impacted when a threat is occurring. The attributes used to define this are the IT asset at risk, CIA (confidentiality , Integrity , Availability) (this defines which principle of security is affected) and Impact

IT asset	CIA	Impact
MS-SIS Informational Assets (mass)	C	Critical
MS-SIS Informational Assets (isolated)	C	High
MS-SIS Business Processes (Mass)	I	Critical
MS-SIS Business Processes (Isolated)	I	High
MS-SIS Business Processes (mass)	A	Critical
MS-SIS Business Processes (Isolated)	A	High
MS-SIS Key Establishment Process (Mass)	C	Critical
MS-SIS Key Establishment Process (Isolated)	C	Moderate
MS-SIS Key Management Process (Mass)	I	Critical
MS-SIS Key Management Process (Isolated)	I	High
MS-SIS Operational Assets Inventories (Mass)	C	Moderate
MS-SIS Operational Assets Inventories (Isolated)	C	Low

Likelihood of attack by specific threat agents:

We now define the likelihood of a threat agent putting an asset at risk, the attributes used to define this are the threat agents, the likelihood that the threat agent is both an insider or an outsider.

Threat / Threat agent Objective	Outsider Likelihood	Insider Likelihood
MS-SIS Informational Asset	Critical	High
MS-SIS Business Processes	High	High
MS-SIS Keys	Critical	High
MS-SIS Operational Assets	High	Moderate
Hackers	High	Moderate
Foreign hackers	Moderate	Low
Corporate spies	Moderate	Moderate

Vulnerability Assessment:

The vulnerabilities are found based on the assets and threat agents, this is done from the flow diagram. The assessment of vulnerabilities is derived by analyzing what the threat agents are likely to go for and how serious its consequences are.

From the functional flow diagram discussed above we can find out how the users connect with the system and determine where the threat agents are likely to be interested in attacking. The vulnerable areas in the **MS-SIS** are mainly the Upload and viewing process as these involve the information assets of **MS-SIS** in transmission. The other are that a threat agent can target is the Key encryption process as choosing a secure key is difficult and is one of the easiest areas for a threat agent to target, this could lead to a critical impact on the company based on the motive of the threat agent.

The actual storage for **MS-SIS** though a very challenging problem, is not the direct responsibility of Marvel Studios as we have decided to go with public cloud storage, careful thought is put into the selection of the cloud service. For the user agents in the **MS-SIS** we use a role based access control for the users to access the Secure Image Solution system using the **MS-SIS** Local application that is installed in the local system, this is also a very vulnerable area for the threat agents to target, the MS-SIS local application must be secure against the threats that might be posed to obtain the assets of Marvel Studio's for intended use.

Further, the usage of a public cloud service also reduces the vulnerabilities of authentication or the quality of protection.

Threat / Threat agent Objective	Vulnerable Areas	Comment
MS-SIS Informational Asset	**MS-SIS** (C) (I)	Accessing the Informational assets would mean the whole system has been compromised
Upload/download failure	**MS-SIS** Business Process (A) (I)	The attacker will try to deny or spoof the connection to make it look like it is geniune
Hackers (DOS)	**MS-SIS** Business Process (A) **MS-SIS** (A)	The hackers may try to target the Business process to prevent the user agents from accessing it
Stealing MS-SIS Keys	Key Management Store (C) (I)	The threat agents are most likely to target the Keys used by the user agent
Corporate spies	**MS-SIS** (C ,I, A)	Corporate spies hired by other agencies might target the whole system to either collapse the system, compromise integrity or deny availability

We now design a table to merge where the attack might take place and what the target is , the attributes for the table are Asset at risk, how it affects the system, the impact it causes, the threat it poses , the vulnerable area in the system and the likelihood of the threat taking place.

IT Asset at risk	CIA	Impact	Threat	Vulnerable Area	Likelihood (O=Outsider , I=Insider)
MS-SIS Informational Assets (Mass)	C	Critical	Steal	**MS-SIS**	Critical (O) High (I)
	I	Critical	Hacker		Critical (O) High (I)
MS-SIS Informational Assets (Isolated)	C	High	Steal	**MS-SIS**	High (O) Moderate (I)

	I	High	Hacker		High (O) Moderate(I)
MS-SIS Business processes(mass)	A	Critical	Hacker (DOS)	Business Process	Critical (O) High (I)
	I	Critical	Hacker		Critical(O) High(I)
MS-SIS Business processes (Isolated)	A	High	Hacker(DOS)	Business Process	High (O) High(I)
	I	High	Hacker		Critical (O) High(I)
MS-SIS Keys(mass)	C	Critical	Steal	Key management store	Critical (O) High (I)
MS-SIS Keys (Isolated)	C	Moderate	Steal		High (O) Moderate(I)
MS-SIS Operational Asset Inventory (mass)	C	Moderate	Steal	**MS-SIS**	Moderate (O) Low(I)
MS-SIS Operational Asset Inventory (isolated)	C	Low			Low(O) Low(I)

From the above tables, we can now determine how different threats affect the system and then prioritize the threats so that we can decide which threats to acknowledge first thereby decreasing the risk.

Threat	**Impact**	**Likelihood (O= Outsider , I=Insider)**	**Risk Priority**
SIS Key Establishing Process (Mass)	Critical	Critical(O) High (I)	1
MS-SIS Information Assets (Mass)	Critical	Critical(O) High (I)	1
MS-SIS Business Process(mass)	Critical	Critical (O) High(I)	1
SIS Key Establishing Process (isolated)	High	High (I OR O)	2

MS-SIS Information Assets (isolated)	High	High(O)	2
MS-SIS Informational Assets (Isolated)	High	Moderate(I)	3
MS-SIS Business Processes (Isolated)	Moderate	High (O or I)	3
MS-SIS Operational Assets(Mass)	Low	Moderate(O) Low(I)	4
MS-SIS Operational Assets (Low)	Low	Low(I or O)	4

Security Engineering:

This section deals with the requirements that were specified in the start of this document and the risks that may occur that might involve the requirements failing. By considering this, we get the security requirements for the **Marvel Studio – Secure Image Solution (MS-SIS)** system

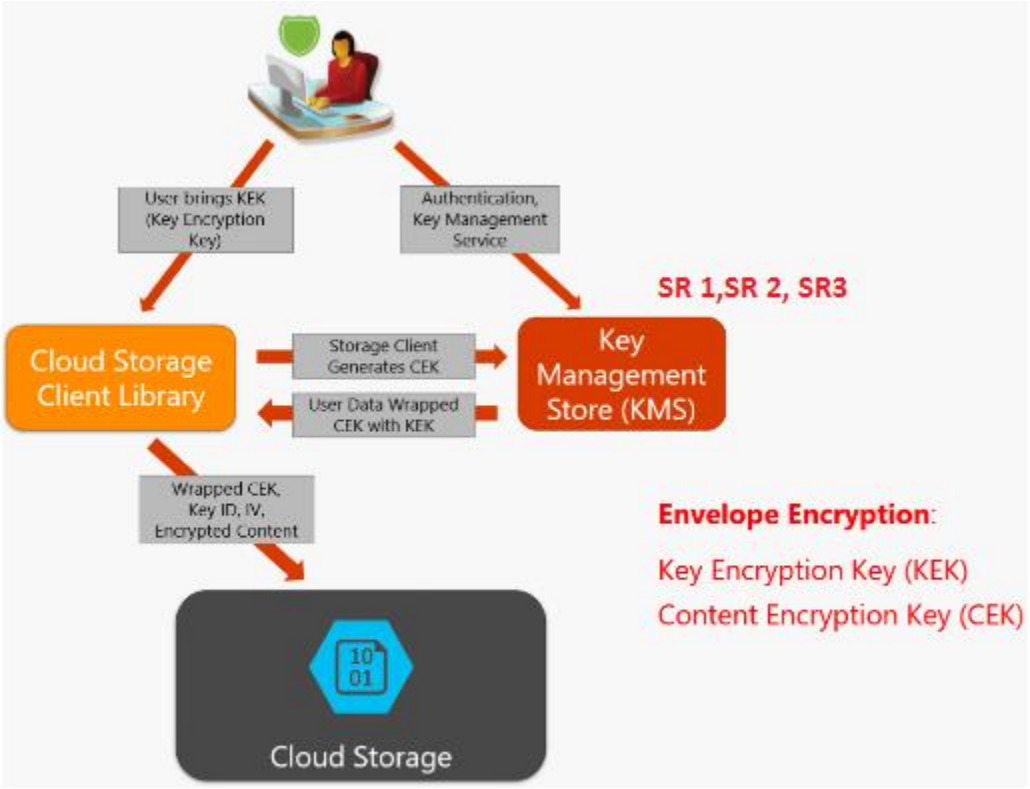
Threat	**Impact**	**Likelihood (O=Outsider , I=Insider)**	**Risk Priority**	**Security Requirements**
SIS Key Establishing Process (Mass)	Critical	Critical(O) High (I)	1	SR 1: The key must withstand common decryption techniques (Brute force for example) SR 2: Keys must not be stored in an encrypted format. SR 3: Keys must be changed regularly

MS-SIS Information Assets (Mass)	Critical	Critical(O) High (I)	1	SR 4: The Asset can only be accessed by authorized personnel SR 5: Use access control so that only user agent's data can be accessed. (for system admin) SR 6: Provide immutable logging for all access SR 6a: Regular audits of access logs SR 6b: Strict background checks of system admin SR 7: Protect confidentiality of data on transit (network links) SR 8: Constantly backup data
MS-SIS Business Process(mass)	Critical	Critical (O) High(I)	1	SR 9: Protect all connections to block known attacks SR 10: Use secure application software configurations SR 10a: Maintain Security patches for application software

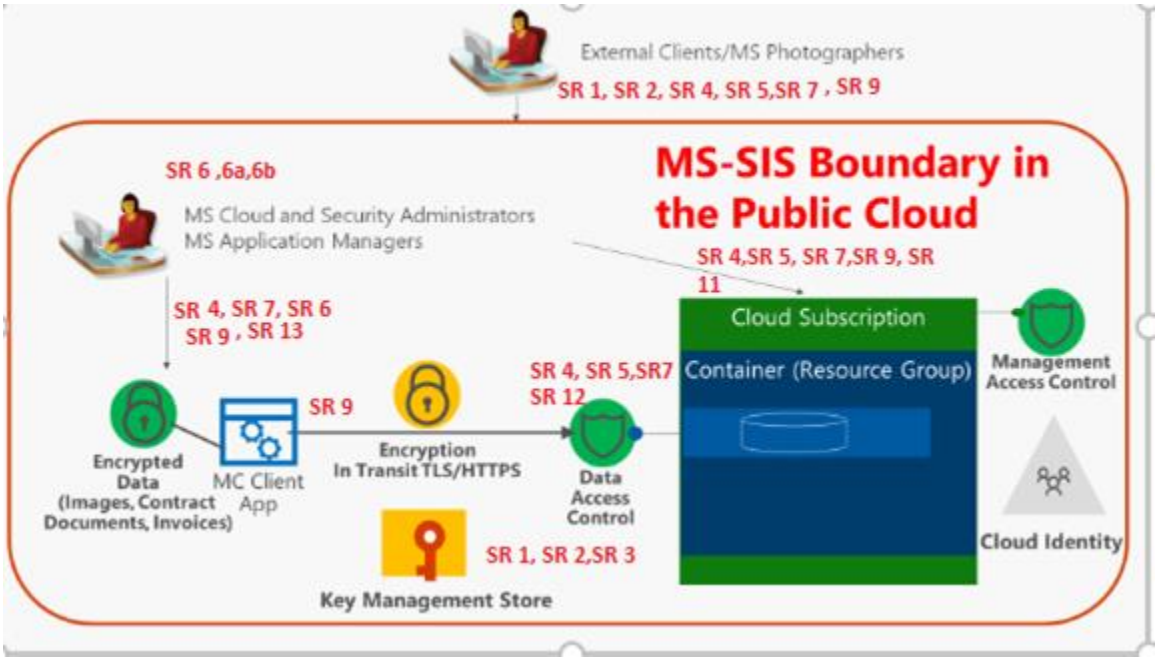
SIS Key Establishing Process (isolated)	High	High (I OR O)	2	Already dealt with by SR 1, SR 2, SR 3
MS-SIS Information Assets (isolated)	High	High(O)	2	SR 11: Data must be securely encrypted before uploading SR 12: Each log in by user agent must be logged.
MS-SIS Informational Assets (Isolated)	High	Moderate(I)	3	Dealt with by SR 4-8 and SR 11, SR 12
MS-SIS Business Processes (Isolated)	Moderate	High (O or I)	3	Covered in SR 9, 10
MS-SIS Operational Assets Inventory(Mass)	Low	Moderate(O) Low(I)	4	SR 13: The asset (inventory) must be regularly checked for unauthorized changes
MS-SIS Operational Assets Inventiry (Low)	Low	Low(I or O)	4	Covered in SR 13

Security Assessment:

We can now show where the security requirements are needed in the **MS-SIS** by mapping the security requirements onto the flow diagram



A much clear idea can be obtained by mapping the requirements on to the system boundary diagram



In this section, the security requirements will be compared with the new system to see if all the requirements are satisfied. The first requirements deal with key security, the keys must be resistant against common attacks, and the keys must be rotated/changed regularly to make it harder for the threat agents to attack the system. The requirement SR 4 was to restrict access only to authorized personnel, one of the changes being established in the new system is to make it a role based access system, which means a specific user agent can only access their own information and the data that they have uploaded and only data that is meant for them. This solution also deals with SR 5 which requires the system to have access control for data to be accessed only by the respective user agent. The next requirement SR 6 is used to prevent repudiation and is also helpful for the organization audit and has credibility.

Marvel Studio – Secure Image Solution uses a secure local application to connect to the public cloud, in this application programmers must make sure that the data that is being transferred through the public network is secure i.e., the data must be secure even when in transit. This takes care of the requirement SR 7. The requirement SR 8 is very important because in case of a catastrophe to the cloud server, the data will all be lost if not for a backup. The next requirement SR 6 deals with protecting all the connections to block common known attacks, this can be done by adding filters or firewalls. The application software for the MS-SIS must use secure configurations which include network protocols used and other attributes. The Security of the application depends on the programmers and security patches must be released regularly to keep it updated and secure against the ever-challenging threats.

Trade Study:

MS-SIS uses a thick client application for the external users or can be accessed using the web browser. For the other user agents who are part of the **MS-SIS** the system is accessed either by using the web browser or through cloud based back end access. In this section, we discuss how each interface that is chosen for the **MS-SIS** fare against various deciding criteria like Security, Maintenance Cost, Initial Cost, Ease of use. Each criterion is evaluated for each user agent's interface to see how it compares against each interface option. The rating is done on a scale of 1 to 4 where 1 = Poor, 2 = Moderate, 3 = Good ,4 = Very Good. The total score is calculated as the average of all the criteria and the interfaces which cross the threshold are given a total score of 0.

For external users:

Criteria	Web Browsers	Thick Client	Cloud backend access
Security	3	3	4
Initial Cost	4	2	4
Maintenance Cost	3	2	1
Ease of use	4	4	1
Total Score	3.25	2.5	0

For external users, the only data that must be securely transmitted are the pictures and that is for the purpose of viewing, the application must be easy to a user hence the cloud back end access is not right for an external user. The best choice for an external user would be either by using the **MS-SIS** Local application or by accessing using a web browser. The better

For Photographers, System Admin, Application Managers:

Criteria	**Web Browsers**	**Thick Client Application**	**Cloud backend access**
Security	3	3	4
Initial Cost	3	3	4
Maintenance Cost	3	1	2
Ease of use	4	4	2
Total Score	3.5	0	2.8

The main Business Process of securely uploading and storage of informational assets, maintenance of **MS-SIS** system, bug fixes and audits are done by the user agents specified above, the main requirement for these user agents is security, all the interfaces are pretty secure. The next concern would be the maintenance cost, the cost of maintaining a client application is very large and for a company which is just rolling out its technology, the technology team decided to not go through with thick client application and rather use a browser based approach which connects to the **MS-SIS** Securely. The other option, Cloud backend access is much faster to use for a user agent with the knowledge of how to use it and very secure.

Guiding principles

This section will summarize the principles the company will adopt in order to achieve the goals.

We use the guiding principles as suggested by RSA Executives who offer seven guiding principles to maximize megatrends redefining the information security industry:

1. Security must be embedded into the IT Infrastructure
2. Develop ecosystems of solutions
3. Create seamless, transparent security
4. Ensure security controls are correlated and content aware
5. Security must be both outside-in and inside-out focused
6. Security has to be dynamic and risk-based
7. Effective security needs to be self-learning

Guiding Principle 1: Security must be embedded into the IT infrastructure

Information Security is the single most important aspect of the organization. It doesn't necessarily have to be our online trace, but also the physical security threats that exists such as copies of our records that we leave behind. The security risk is even more amplified because we do not have only employees, but outside vendors, contractors, mobile workers etc which pose more security threat to any organization. Risk management because a critical issue here and as mentioned earlier in our goal, to mitigate much of our security issues, we have appointed a Chief Information Security Officer (CISO) who can do effective security management of the organization.

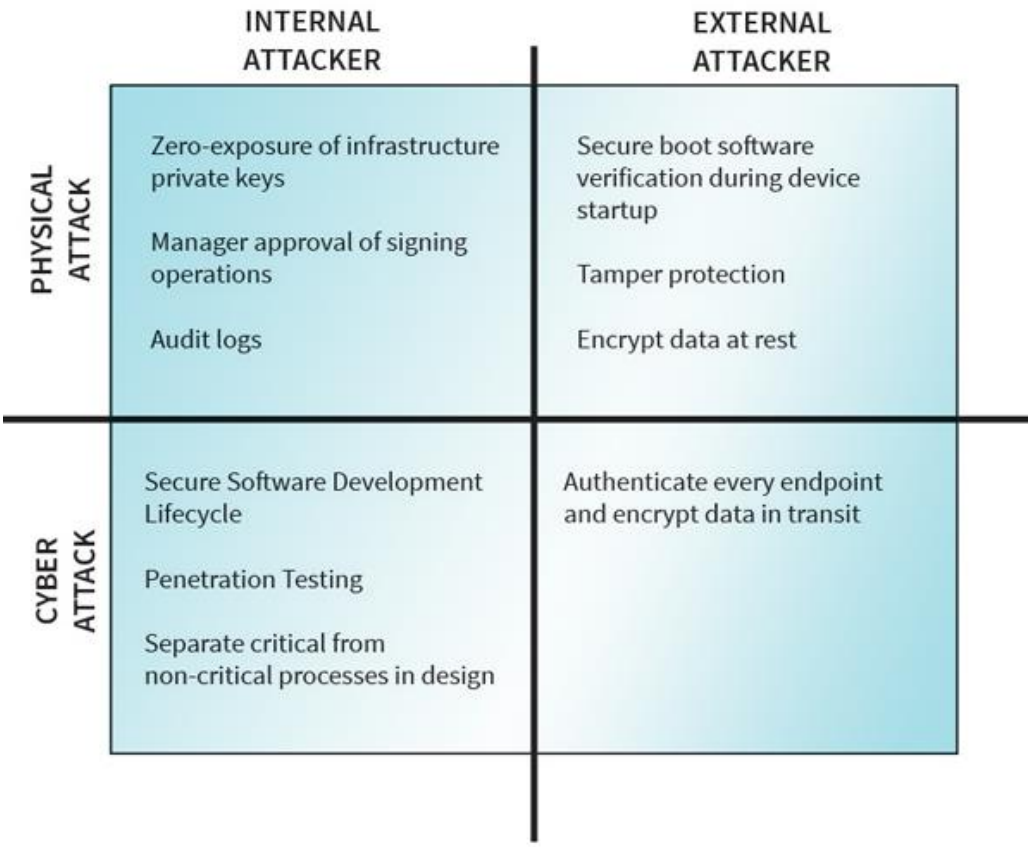
We need to make sure that we are not using operating systems for critical IT needs that are obsolete, vulnerable, and yet connected to the internet, increasing the likelihood of the security incident.

It is essential not only to have smart protection systems on the devices that hold or access them but also to and further barriers such as encryption and multi factor authentication, as well as sound network segmentation and reliable incident recovery strategies.

We need to have built in security to the infrastructure since we cannot reply on other devices' security, the IT system must be designed for confidentiality and authentication which includes cryptographic algorithms and a security infrastructure.

We need to account for the following things:

1. The importance of Keys – We need to use a Public Key Infrastructure for end to end encryption.
2. End-to End Security Design – We need to account for both internal and external attackers when it comes to the security for our system. Designing a secure embedded system means planning and mitigating threats across the entire product life cycle.



3. Enterprise Security Infrastructure – End to End Security extends beyond the device, addressing the key management infrastructure required for manufacturing and maintenance.

We need to ensure that Data Loss Prevention mechanisms are implemented in the system itself.

Guiding Principle 2: Develop ecosystems of solutions

We need to develop a system such that the core components of the system can be complemented by applications made by other companies.

This principle involves the following

1. Challenging how to develop IT solutions
2. Leveraging the power of IT ecosystem instead of trying to do it
3. Developing IT solutions that meet future requirements
4. Finding compatible technology that perfectly integrates with your IT solution
5. Fostering collaboration to create IT value
6. Taking IT technology for a test drive before many any purchase decisions

Guiding Principle 3: Create seamless, transparent security

The security of the system should be built in such a way that the users – all kinds of users can understand the security mechanism behind the IT solution. To create transparent and seamless security we need to ensure that if some mechanism is in place, that mechanism can easily be adapted in advanced technologies. In this changing IT technology, where new innovations are just around the corner, our system should be designed in such a way that it can adapt to changes.

To create transparent and seamless security, the following needs to be done:

- Support Transparency on Multiple Levels
- Automate Vital Security Processes
    - Automated Protection
    - Improved Authentication Mechanisms
    - Hardware Based Encryption
- Administer Security from a Central Point
    - Centralized Data Security Administration
    - Controlled User Access
    - Wide Ranging Device Support
- Adapt Security Policies to Include Emerging Technologies
    - Emerging Technologies – cloud computing, smartphones/tablets usage at work
    - Vigilant Security Practices
    - Regular Re-evaluation
- Adopt an Operating System Agnostic Approach
    - OS independent Security Mechanisms
    - Security at a Pre-Boot Level

An example of a company doing this, is Google. In the Next'17 cloud conference, Google made seamless security the highlight of the conference. Some of the things they are doing to make security seamless are:

- Physical Security – in additional to the surveillance cameras, iris scanners and motion sensors, metal detectors, Google has added that each data center has more than 175 physical security guards.
- Google is building its own hardware systems so that they have full visibility into its global supply chain and know where each part came from
- Google unveiled a custom Google designed Trusted Platform Module – Titan. This Titan is used to authenticate software installed on hardware, including BIOS software. This module is also able to check if the log has been tampered by using a monotonic counter
- Google authenticates users at application level through and makes use of tools which trusts users rather than networks
- Google has made Data Loss Prevention a seamless and an automatic process by letting companies create filters to prevent SSN being sent by email by scanning emails for both – inbound, outbound traffic, message body and attachments
- Creation of Data Loss Prevention API – which can redact all sensitive information from text or images and is integrated into Google Technologies such as GSuite
- Google Vault Service – seamlessly integrated into its cloud offerings
- Two-factor authentication for GSuite applications is accessed from some place where you haven't accessed before.

Guiding Principle 4: Ensure security controls are correlated and content aware

We need to make a centralized security information management system so that we can correlate data from information controls such as risk based authentication. A content aware security means that the IT system has the ability to understand the contents of the data itself. This means that we should implement security in such a way that it protects sensitive data automatically against modern threats.

Following this guiding principle will protect us from insider threat since this principles states that the security controls in place should be able to detect if any unauthorized access is being done and be able to prevent this from happening. This prevents unwanted behavior form either employees or vendors.

Example of a company providing such a solution is – Digital Guardian which claims to be the only content aware security solution which offers continuous monitoring and complete visibility. They provide services such as:

1. Application Control
2. Compliance
3. Data Classification

4. Device Control & Encryption
5. Email Control & Encryption
6. Insider Threat Protection
7. Malware Protection
8. Memory Forensics
9. Privileged User Control
10. Ransomware Protection
11. Trusted Network Awareness
12. Web Apps & Cloud Storage Control

Guiding Principle 5: Security must be both outside-in and inside-out focused

Security breach can happen due to insider threat agents or outsider threat agents. Previously, the focus on preventing security breaches outside-in thinking that there is more harm from outsiders than insiders. However, nowadays, it has come to realization that much of the security breaches can happen due to insider threats as well. An example of such an incident is the NSA leaks by the former employee, Edward Snowden.

In order to mitigate ourselves from all possible threats, we need to focus on security that is both outside-in and inside-out focused.

We need to do this by having controls in place for insider access as well. A much security threat to organizations these days is usage of personal devices at work. Usage of personal devices can cause much harm to any company if it is done intentionally by employees to cause harm to the system.

If any company allows usage of personal devices at work, then policies must be set for usage of personal devices. Besides having security controls only for using personal devices, one must also have security controls in place for employees, vendors etc. accessing the system.

Some guidelines that be enforced in using personal devices are:

- Do not use personal devices without getting prior approval from the manager
- Use an encrypted USB device if you need to use one
- Do not use private emails at work
- Send documents in encrypted form – password protected
- Do not use work emails in your private devices

Guiding Principle 6: Security has to be dynamic and risk-based

We need to implement security controls and mechanisms depending on the functionality of our assets. We need to do a security risk analysis on all of our critical Information Assets and once that is done, we need to implement security controls in place accordingly.

We need to have dynamic access control so that each access request is based on the risk of such an access in operational level. Instead of having traditional access model where if you have the credentials, you can access the system, access should be controlled in real time basis.

Examples of implementing dynamic and risk based security include using fuzzy logic which uses a percentage matching algorithm to authenticate a transaction. Depending on the logic and percentage matching, if something matches 80% of the restricted value, then the transaction is not allowed. A real-life example of this when you do a transaction in the bank, and send money to someone. Your name is checked against the OFAC list which is the list of blacklisted people in Office of Foreign Asset Control. If your name matches 80% to the names in the list, then you will be automatically restricted from doing the transaction until further investigation is done. This is an example of a dynamic and risk based security control in place.

Other ways of implementing dynamic and risk based security are – Machine Learning, Probabilistic Inference, Decision theory etc.

Guiding Principle 7: Effective security needs to be self-learning

We need to implement security controls in any organization but once we have implemented it, we need enforce in such a way that we do not need to repeatedly tell someone to do something. We need to implement artificial intelligence in our security solutions so that if an unpredictable behavior is detected, our system will be able to detect this pattern, and implement security controls accordingly.

Examples include Cisco's Self Learning Network (SLN) which is able to analyze the network traffic and detect if there are any anomalies in the network.

Goals

This section will include the statement of the mission and strategic goals/objectives of Information Security for the company.

This section will include the statement of the mission and strategic goals/objectives of Information Security for the company.

Mission Statement: The mission of MS-SIS is to deliver a secure image solution to all the users while protecting

Strategic Goals

Goal 1	Protect the confidentiality of the data
Goal 2	Preserve the Integrity of Data
Goal 3	Improved Security of System and Network Services
Goal 4	Proactive Risk Management
Goal 5	Crisis and Security Incident Management

Goal 1: Protect the Confidentiality of the data

Confidentiality is an integral part of any organization. We need to make sure that the data that we have is not accessed by someone who doesn't have the right to do so. Similarly, for MS-SIS, we need to maintain confidentiality of the data, not only from outsiders but also from users inside the organization. Not everyone needs access to everything.

In order to do so, we need to have policies in place for Role Based Access Control. For our MS-SIS, we will design our system in such a way that users have aces on a need to know basis. The authorized access to any part of the system will be carefully designed.

This data not only pertains to the information that is stored online but also relates to the physical copies of the data that we may have. Since, all of the images are digitally scanned in the system, we will retain hard copies and set policies in place for storing, scanning and disposing of the data stored online and offline both.

Goal 2: Preserve the Integrity of Data

This means that non-authorized users should not be able to modify the information that they do not have access to. This means that the data should not be added, changed or deleted. We need to make sure that the data isn't changed and need to make sure that data changes and any violation of data can be detected. We need to have an audit trail log in order to check who did what in the system. This also corresponds to our Goal no 1 which is unauthorized access of data. An audit trail will be able to satisfy both of our goals. But of course, this is not the only thing that can be done. Other control measures should be in place as well in order to preserve the integrity of data.

Goal 3: Improved Security of System and Network Services

Since, we migrated to a centralized system, our main goal is also to provide improved security of the system and network services. We will do a monthly penetrating and vulnerability testing internally to check the security of our system and network services. By doing this if we potentially find some threats then we can mitigate it by timely detection and applying the fix to do that. Once we strengthen our security testing, our system will automatically have improved security. Also, additionally, we will also be doing external audit so that we have an idea of how secure our system is from a third-party point of view. By doing this on a consistent basis, we will aim to have an improved security of system and network services.

Goal 4: Proactive Risk Management

We need to do proper risk management in place to identify the risks associated with the security of the system, analyzing the risks and deciding how to manage the risks. To do a risk management, we can do either a qualitative or quantitative risk analysis. We have mentioned the security risk associated with our system in the earlier section where we have identified the potential risks and vulnerabilities, and the security requirements needed to mitigate the risk. In order to do this also, we need to have policies in place related to our security such as IT Risk Assessment and Management. We need to have risk assessment to know the risks associated with the potential threat and vulnerabilities in our system. Similarly, we need a Risk Management Policy related to IT Security so that we can have policies in place for all the risks associated with our system. This follows in our Goal 5 which specifically focuses on crisis and security incident management which focuses on an event where as this, focuses on creating policies to mitigate any potential risks identified in Risk management process.

Goal 5: Crisis and Security Incident Management

The risk of cyber threat is so severe now that, we need to have controls in place in case a major outbreak occurs. We need to have mechanisms in place so that if there is a detection of any kind of potential crisis, everyone knows what to do. For this purpose, we need to have someone to lead the IT Security Team and a responsible person who can be in charge of this and all IT Security issues, namely the Chief Information Cyber Security Officer. This person will be in responsible for having policies in place for potential Crisis and Security Incident Management which will need to be approved by the board.

Policies and Procedures – Guidelines for making them

In order to fulfill our goals, we need to make certain policies and procedures in the organization and make sure that they are enforced.

Development of Policies

For each of the policy that we need to make in order to reach our goal, the policies must be made by the following steps:

We must develop policy an implement in a way so that it will help the organization. However, the way we develop it can either help or hinder its usefulness. The policy is only enforceable if it is designed properly, developed and implemented using a process that assures good results.

Our approach has the following six strategies to implement the principles that the company needs to adopt:

1. Developed using industry-accepted practices
2. Distributed or disseminating using all appropriate methods
3. Reviewed or Read by all employees
4. Understood by all employees
5. Formally agreed to by act or affirmation
6. Uniformly applied and enforced

To develop an information security policy, the following are the phases of the development of the policy

1. Investigation Phase
2. Analysis Phase
3. Design Phase
4. Implementation Phase
5. Maintenance Phase

Once the information security policy is developed, then we need to implement the following phases

1. Policy Distribution
2. Policy Reading
3. Policy Compression
4. Policy Compliance
5. Policy Enforcement
6. Automated Tools

Additionally, we need to

1. Gather Key Reference Materials
2. Define a Framework Policies
3. Prepare a Coverage Matrix
4. Make Critical Systems Design Decisions
5. Structuring Review, Approval and Enforcement Processes

Governance model

This section should include how the information security organization will be structured to address all security functional areas.

For a company to function correctly, it needs three components, one to make all the decisions, one to implement all the said decisions and the third is for communication which is important in a project as people interact with other people. Thus, the three components of the governance model for Marvel Studios used for the **MS-SIS** System are:

1. Decisioning Structures:

The decisioning structure for **MS-SIS** System cannot be given to the same group that takes care of **Marvel Studios's** decision making. The decisions for **MS-SIS** cannot be given to the stake holders and other non-technical members who maybe in the decision-making structure of Marvel Studios. The decision-making authority of **MS-SIS** is given to the CIO, under whom come the Project manager, Security administrator, System administrator and few high-level members of the design team.

The team chosen for the Decision structure will be responsible for all decisions for the **MS-SIS** system. The group consists of all the departments that would be responsible for the proper functioning of the **MS-SIS** system. The CIO would be responsible for considering the impact of the decisions made for **MS-SIS on** Marvel Studios. The project manager is present to determine and for their expertise on the **MS-SIS** which would help in better decision making. The administrators are present to give them a better idea on the details of the project and what they must do as they don't have a major team. The design team-members are present to determine the requirements based on the decisions and needs.

2. Operating Procedures:

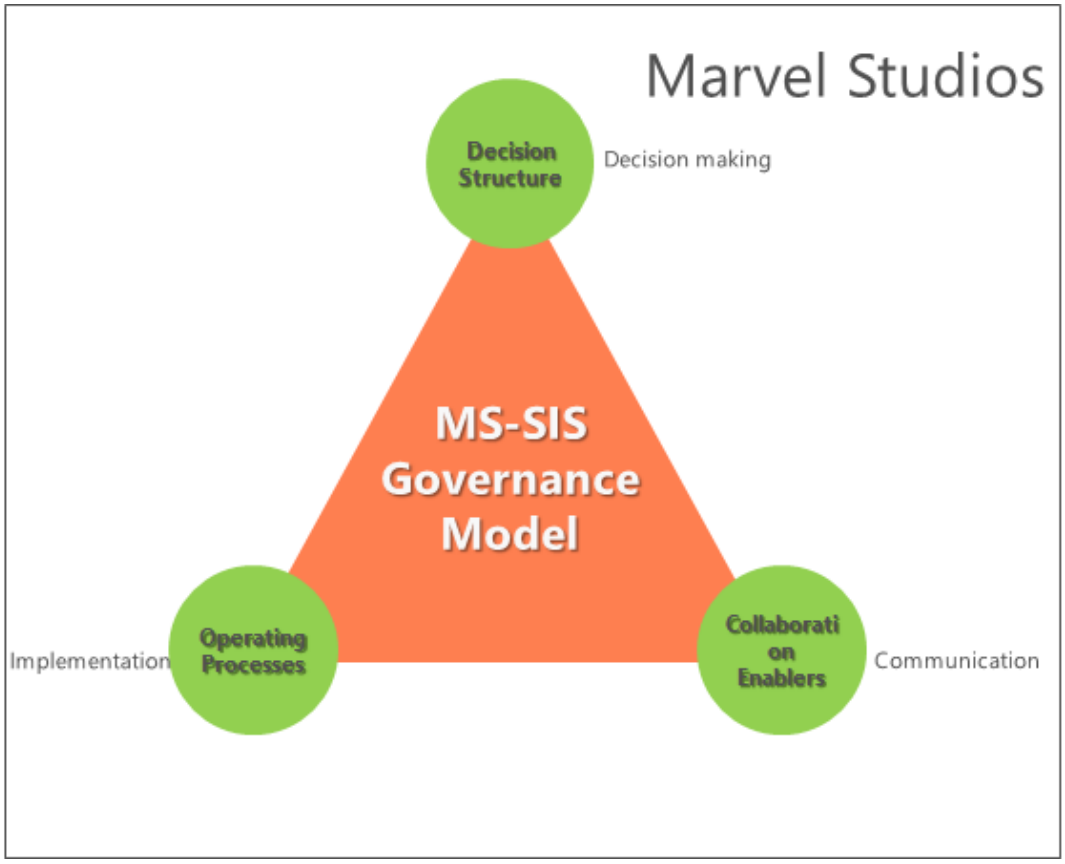
This component is used to define how the decisions are carried out into results. The simple and effective way to determine this is to divide the actions needed to process. These processes are distributed based on the role of the team by the project manager. Some of the basic minimal processes can be

- Have a plan to achieve results (plan management).
- Work with other teams (interdependency management).
- Remove obstacles that impede progress to the plan (issue management).
- Avoid risks (risk management).
- Manage scope boundaries (scope management).
- Communicate to departments (communication management).

The Project manager is responsible for making sure all these processes are done effectively. The project manager then assigns processes to each department that is responsible and gets regular updates on the status. The project manager is also responsible for communicating any important information like bugs, reports etc., to the management in between the regular meeting, the project manager makes the system functional. The project manager is also responsible for quality control and to determine if all the requirements are met and the decisions carried out before each meeting.

3. Collaboration enablers

This section is used to determine how the different members belonging to Marvel Studios communicate. This is basically the bridge between the decisioning and operating procedures. Though this is not necessary, this provides a good guideline and procedures to follow in case of unexpected situations. This is also helpful in case the user set is very diverse, this could give an idea of how the users must be linked and what the communication boundary should be till.



Compliance & Management of Deployed System (Applicable)

ISO/IEC 17799:2005 contains several best practices of control objectives and controls in the many areas of information security management…We are focusing on the 10 of the following areas in terms of MS-SIS System, where they are applied in the MS-SIS SYSTEM.

1. **Security policy**: For the MS-SIS System, we have already discussed and defined various security policies applied.

2. **Organization of information security**: The Marvel's Chief Information Officer (CIO) is responsible for establishing, maintaining, implementing, administering, and interpreting organization-wide information system security policies, standards, guidelines and procedures. While responsibility for information systems security on a day-to-day basis is every employee's duty, specific guidance, direction, and authority for information systems security is centralized for all of Marvel's Information Technology (MSIT) department.

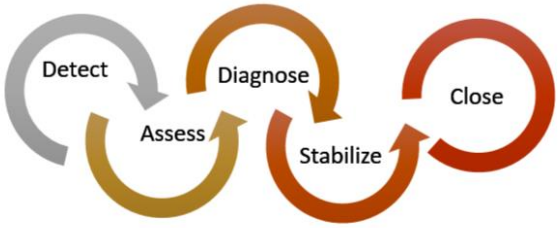
3. **Asset management**: From the Security Requirements, Mobile Device Management for PCs, Laptop and mobile devices like iPad, Android Tablets for External Users. This is used to apply corporate policies on the remote devices. Patching and configuration management are couple of important use cases.

4. **Physical and Environmental security**: **Limited Access to Physical Datacenter**: The physical location of the datacenters and region is guarded by outer and inner perimeters with increasing security at each level, including perimeter fencing, security officers, locked server racks, multifactor access control, integrated alarm systems, and around-the-clock video surveillance by the operations center.

5. **Communications and operations management**: **Audit Logs and Audit verification for certifications such as ISO 27001 by 3rd party**: All of the data access by Cloud Provider's employees and/or subcontractors must be logged all the time. JIT and JEA are in place but we also have to make sure several other security controls are in place like one mentioned. And time to time they must be verified to keep the security controls verified.

6. **Access control**: For MS-SIS, Access Control Policy to our corporate (and cloud based) network is essential to maintain our Marvel Team's productivity, but in many cases this access control issues originates from internal and external networks that may already be compromised or are at a significantly lower security posture than our corporate network. MS-SIS Access Control Policies are defined to mitigate these external risks the best of our ability.

7. **Information systems acquisition, development and maintenance**: The following software modules will be developed internally for MS-SIS: Front End Web Servers, Data Analytics & Reporting, MS-SIS Systems Application.
8. **Information security incident management**: MS-SIS System using a popular public cloud vendor such as Microsoft offer that offers a total security incident management for the platform. Security Incident Roles and Responsibilities are included in the platform.



Reference: https://gallery.technet.microsoft.com/Azure-Security-Response-in-dd18c678

9. **Business continuity management**: MS-SIS SYSTEM will be deployed on the cloud platform and will include a state-of-the-art BCDR (Business Continuity and Disaster Recovery) solution in place. We have covered this as a part of our security requirement, Business Continuity and Disaster Recovery for application backup and overall site DR strategy.

10. **Compliance**: We are making sure that cloud platform by Microsoft (Azure) is fully compliant with the required regulatory agencies such as HIPAA/HITECH, PCI-DSS etc. MS-SIS SYSTEM will be leveraging those compliance certifications.

Reference: https://www.microsoft.com/en-us/TrustCenter/Compliance/default.aspx

Policy Enforcement for authentication and authorization

Let's understand the user and roles within MS-SIS SYSTEM.

I. **The Marvel's Chief Information Officer (CIO)** is responsible for establishing, maintaining, implementing, administering, and interpreting organization-wide information system security policies, standards, guidelines and procedures. While responsibility for information systems security on a day-to-day basis is every employee's duty, specific guidance, direction, and authority for information systems security is centralized for all of Marven's Information Technology (MSIT) department. This department will perform information systems risk assessment, prepare information systems security action plans, evaluate information security products, and perform other activities necessary to assure a secure information systems environment.

II. **External clients (models and celebrities),** who want to access their profiles pictures/portfolios using public website.

III. **MS Photographers (internal users),** who are responsible for encrypting and uploading the pictures/images to the cloud based solution**.,**.

V. For the MS-SIS SYSTEM, **Marvel's Cloud and Security Administrators** (internal users) are responsible for updating, patching and uploading the new version of the proposed solution including periodic back-up of the data. Additionally, they are responsible designing the access control for MS-SIS SYSTEM's cloud based infrastructure. They have a total internal access to the MS-SIS SYSTEM responsible for running the application in a secure way.

VI. For the MS-SIS SYSTEM, **Marvel's Application Managers** (internal users), are responsible for building the MS-SIS solution including secure Data Storage Solution with high availability (SQL Server or MySQL). They will make sure the right level of access controls are defined for various External Clients as well as Photographers when accessing any video, images, pictures or raw data in a secure way and only specific to their access levels.

Now apart from the above user and classes, there are other roles as well within the Marvel Organization to take care of information system security engineering management. Those include IAM or Identity and Access Management Team, Incident Response Teams, Marvel IT Team and many more. In the following, we will correlate several teams under CIO to map the relevant Access Policy rule.

MS-SIS Identity & Access Management (IAM) include the following:

a. Account administration (creating, deleting accounts)

Within the CIO Organization, there are Identity and Access Management (IAM) Team.

IAM Team is responsible for Account Administration such as User Management i.e. Adding, Deleting Users and Groups along with Assigning roles to the Users.
We have already covered it during our Security Requirements and Policies section.

Identity Multi-Factor Authentication (MFA) - Additional level of security in case of any compromised user name and pass for MARVEL Employees. Multi-Factor Authentication (MFA) using Phone or Smart Card over and above user name and password.

Identity - RBAC - Role-Bases Access Control Module - Provide Just Enough Administration for specific set of Cloud Infrastructure for the MS-SIS System

At a very high level, this is how the permissions would look like.
Identity and Access Team will have the following permissions.

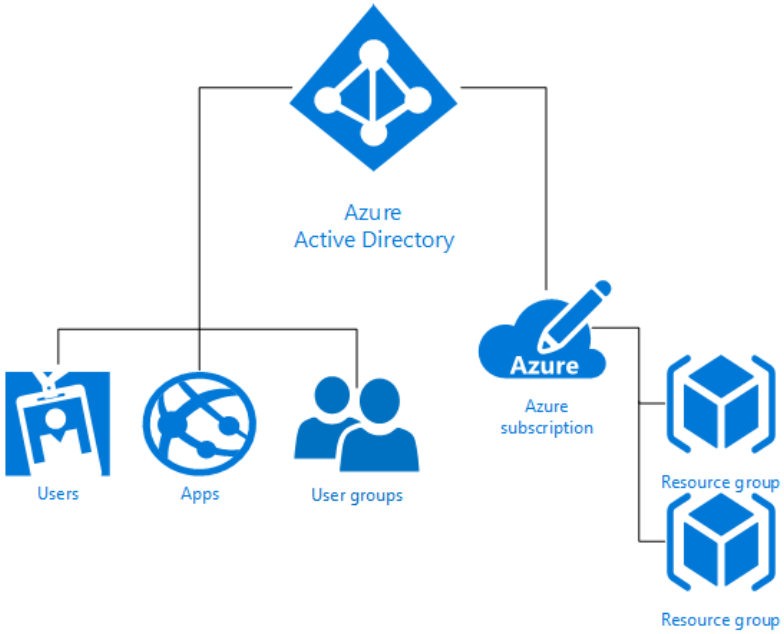
- Create Account
- Update Account
- Delete Account
- Create Group
- Update Group
- Delete Group
- Read Users
- Update Users
- Assign Roles
- Update Roles

MS-SIS SYSTEM relevant users such as the Doctors, the Analytics, the Reviewers and Funders will not have any access to User & Group Management rather than Identity and Access Management (IAM).

All those User Accounts and Groups will be created and maintained by the Marvel IAM Team on regular basis by implementing Multi-Factor Authentication (MFA) mechanism.

b. Access policy (general rules on who should get access to what)

In order to build Access Policy, the Marvel IAM Team will be implementing Microsoft Azure Active Directory (Azure AD) as a solution for Users and Group Management along with MFA support



Reference: https://docs.microsoft.com/en-us/azure/active-directory/role-based-access-control-what-is

IAM Team will leverage and build a Role-Base Access Control Policies. These Custom RBAC Policies will help define, which users within the MS-SIS SYSTEM can have what level of access to the specific resources.

We will have several types or Access Policies (Roles)

- **Owner** (Built-In Role)
  - Complete access to either MS-SIS SYSTEM or specific resources within MS-SIS SYSTEM.
  - Assign access to other users

- **Contributor** (Built-In Role)
  - Complete access to either MS-SIS SYSTEM or specific resources within MS-SIS SYSTEM.
  - Cannot assign access to other users

- **Reader** (Built-In Role)
  - Read only access to either MS-SIS SYSTEM or specific resources within MS-SIS SYSTEM.
  - Mostly for reporting and auditing purpose.

- Cloud Security Manager (Custom Role for MS-SIS_CLOUD_SEC_MANAGER)
  - **Owner** Level Access to Azure Cloud Subscription except customer data or any MS-SIS Studio related data.

- Cloud Application Manager (Custom Role for MS-SIS_CLOUD_APP_MANAGER)
  - **Owner** level access to MS-SIS SYSTEM Application except access to customer data or any MS-SIS Studio related data.
  - **Owner** Update and Patch Management except access to customer data or any MS-SIS Studio related data.
  - **Owner** Manage MS-SIS SYSTEM Resources except customer data or any MS-SIS Studio related data.
  - **Owner** Access to Backup and DR Services except customer data or any MS-SIS Studio related data.

- The Photographers (Custom Role for MS-SIS_PHOTOGRAPHERS)
  - **Contributor** level access to MS-SIS SYSTEM Studio related data such as videos, images, pictures and/or raw data, access to algorithms to the specific set within the MS-SIS SYSTEM database.
  - **No Access** to the MS-SIS SYSTEM Core Application Platform

- The External clients (models and celebrities) (Custom Role for MS-SIS_EXTERNAL)
    - **Contributor** level access to MS-SIS SYSTEM Studio related data such as videos, images, pictures to the specific set within the MS-SIS SYSTEM database.
    - **No Access** to the MS-SIS SYSTEM Core Application Platform

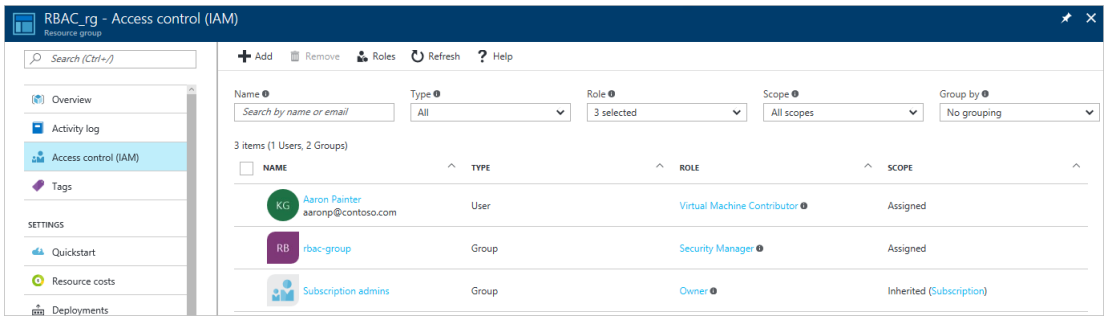
- CIO and CIO Directs (Custom Role for MS-SIS_CIO_ORG)
    - **Owner** Level Access to Azure Cloud Subscription except customer data or any MS-SIS Studio related data.
    - **Owner** Update and Patch Management except customer data or any MS-SIS Studio related data.
    - **Owner** Manage MS-SIS SYSTEM Resources except customer data or any MS-SIS Studio related data.
    - **Owner** Access to Backup and DR Services except customer data or any MS-SIS Studio related data.
    - **Owner** level access to MS-SIS SYSTEM Application except customer data or any MS-SIS Studio related data
    - **No Access** to the MS-SIS SYSTEM customer data or any MS-SIS Studio related data.

- Marvel Identity and Access Management (Custom Role for MS-SIS_IAM)
    - **Owner** Level Access to User Management (CRUD Operation)
    - **Owner** Level Access to Group Management (CRUD Operation)
    - **Owner** Level Access to Role-Creation and Role Assignment.

c. Access rule configuration table development, maintenance and deployment

User Class	**Role**
CIO and CIO Directs	MS-SIS_CIO_ORG
Cloud Security Manager Team	MS-SIS_CLOUD_SEC_MANAGER
Cloud Application Manager Team	MS-SIS_CLOUD_APP_MANAGER
The Photographers	MS-SIS_PHOTOGRAPHERS
External Clients	MS-SIS_EXTERNAL
Marvel Identity and Access Management Team	MS-SIS_IAM

As you can see, we could create built-in table. And within Azure it looks like below.



Reference: https://docs.microsoft.com/en-us/azure/active-directory/role-based-access-control-configure

Security Metrics

We are using Microsoft's Azure a public cloud platform for deploying our MS-SIS SYSTEM. As we deploy the solution within the cloud platform, we have to make sure that the MS-SIS SYSTEM implementation is done by following the specific architecture design guidelines and it is following industry best practices.

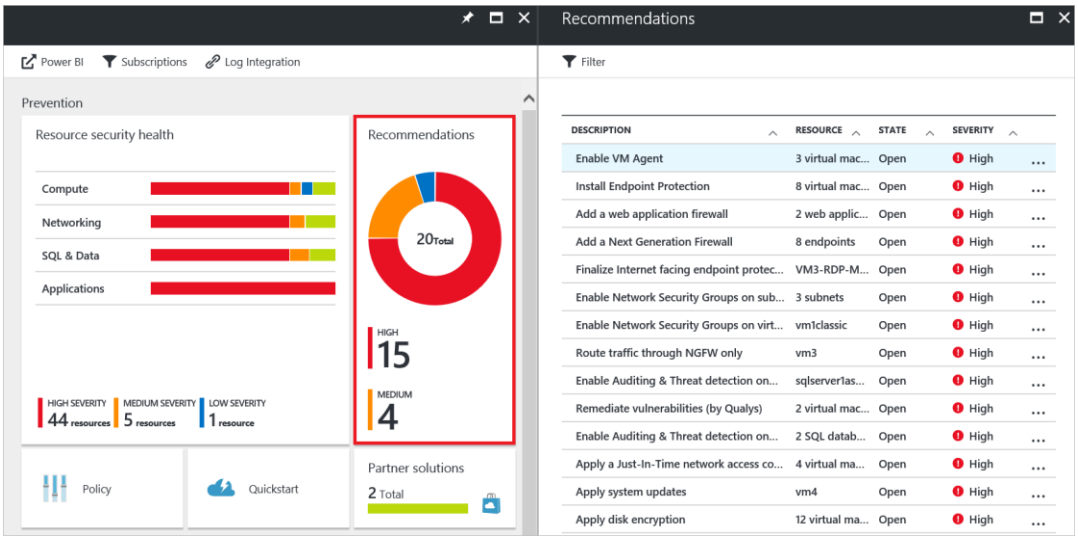
At the same time, we must make sure that we have adequate amount of security monitoring, alerting and diagnostics solution in place. Thus, within Microsoft Azure, we will be leveraging a solution **Azure Security Center.** This will help with the **two key security metrics** within the MS-SIS SYSTEM to support our security. Azure Security center helps organization prevent, detect and respond to the threat. And at the same time, it provides us with the better visibility within the environment and control our security and implement solutions to fix the security issues.

The two-security metrics for MS-SIS SYSTEM are as follows.

- **Security Recommendations**

  When we deploy the MS-SIS SYSTEM and enable Azure Security Center, it analyzes the deployment for potential security vulnerabilities and then based upon the best practices collected so far across the globe it provides the Security Recommendations.

  For e.g.
  - Encryption of the OS and DATA drive if it's missing
  - Missing Antimalware within the operating system
  - Any software Firewall within the Web Application
  - Network security rules or conditions like forwarding/filtering
  - Database related policies and recommendations
  - Auditing and Diagnostics related recommendation
  - Missing System Updates and any OS Configuration changes etc.



Reference: https://docs.microsoft.com/en-us/azure/security-center/security-center-intro

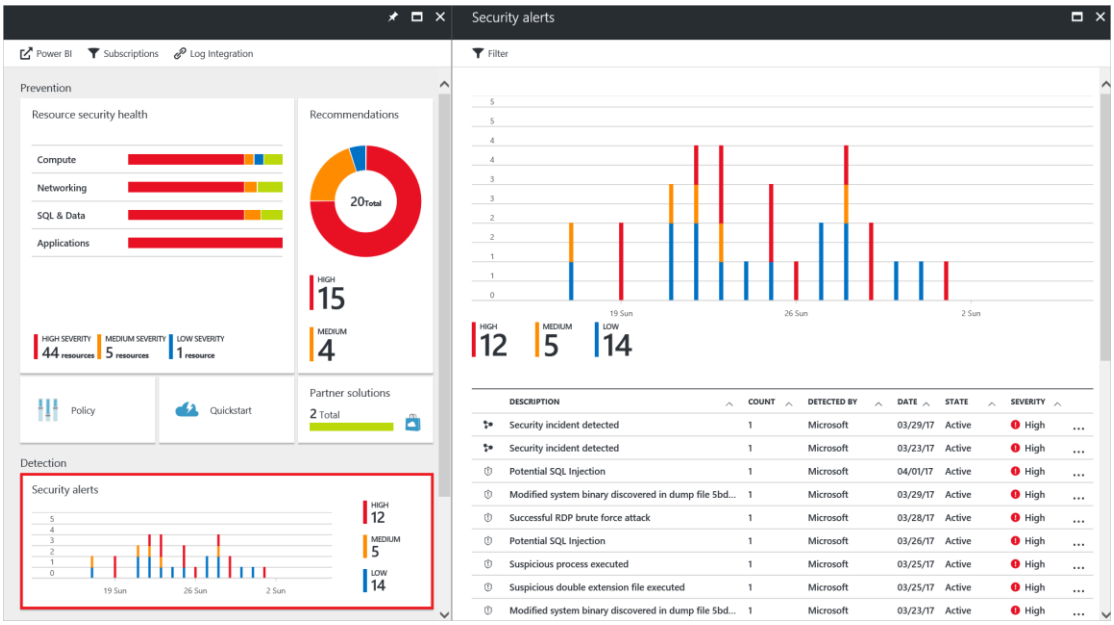
- **Security Alerts**

Once we deploy MS-SIS System in the Azure cloud platform and enable Azure Security Center, it automatically collects, analyzes and integrates all the log data from the Azure Virtual Machines and other artifacts or resources like Network, Storage components, and 3rd party ISV Solutions that you may have deployed within the VM.

Microsoft Azure Security Center then leverages global threat intelligence from Microsoft services and groups like the Microsoft Digital Crimes Unit (DCU), the Microsoft Security Response Center (MSRC), and external feeds. Also, it leverages and applies advanced analytics, by including machine learning and behavioral analysis within the collected data and logs and reports and threats or attacks within your environment.

For e.g.

- Tracking any Brute Force attacks against Virtual Machines
- Any Database related attack like SQL Injection
- Any DDoS type of Attacks on the Virtual Machines
- Any malware detection such as Ransomware or other of its kind.



Reference: https://docs.microsoft.com/en-us/azure/security-center/security-center-intro

Thus, **Security Recommendations and Security Alerts** are the two most important security metrics are implemented by MS-SIS SYSTEM Team within Microsoft Azure to support our security of the MS-SIS SYTEM and its environment.

How would you go about verifying the data you are getting for 3rd party assessment?

- Audit & Diagnostics Logs
- SIEM Tool Integration from MS-SIS Platform
- Penetration Testing/Auditing by Marvel IT Team
- ISO and SOC Compliance Reports
- Trending Analysis (Machine Learning based model)
- Datacenter Tours by 3rd Party Cloud Providers

Assurance

Assurance means the guarantee that our system is doing what it is supposed to do – providing us with the service, and also ensuring that necessary controls are in place. It provides us with the computer security functions such as – Confidentiality, Integrity, Availability, Authenticity, Non-Repudiation and Confidentiality of user data. It uses all – physical, technical and administrative controls to accomplish these tasks.

An example of Assurance is EAL (Evaluated Assurance Level) which defines how well we can trust the product to meet the security defined in the protection profile. Common Criteria calls this a ground for confidence. The rating is from 1 to 7. EAL 1- 4 are Basic Assurance, EAL5 is Medium Assurance and EAL 6-7 is High Assurance.

1. EAL1: Functional Test
2. EAL2: Structural Test
3. EAL3: Methodical Test and Check
4. EAL4: Methodical Design, Test and Check
5. EAL5: Semiformal Design and Testing
6. EAL6: Semi formally Verified Design and Test
7. EAL7: Formally Verified Design and Test

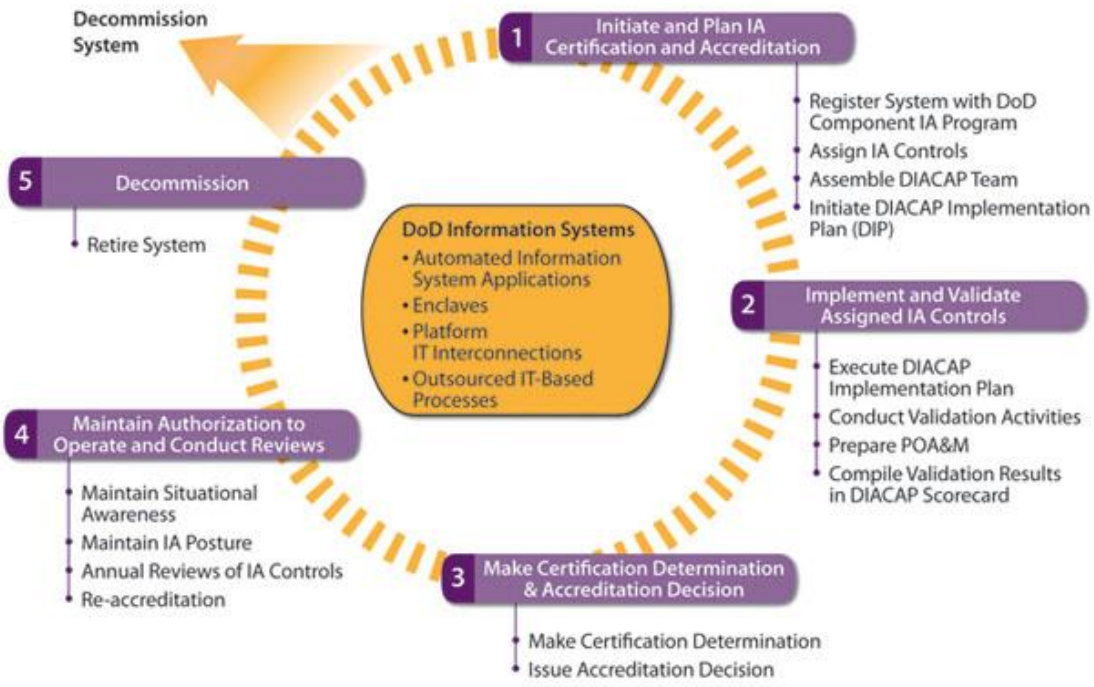
The following is the EAL Level / Robustness Level of the Security Requirements for MS-SIS:

SR 1: The key must withstand common decryption techniques (Brute force for example)	EAL7
SR 2: Keys must not be stored in an encrypted format.	EAL6
SR 3: Keys must be changed regularly	EAL5
SR 4: The Asset can only be accessed by authorized personnel	EAL4
SR 5: Use access control so that only user agent's data can be accessed. (for system admin)	EAL4
SR 6: Provide immutable logging for all access	EAL5
SR 6a: Regular audits of access logs	EAL6
SR 6b: Strict background checks of system admin	EAL4
SR 7: Protect confidentiality of data on transit (network links)	EAL3
SR 8: Constantly backup data	EAL3
SR 9: Protect all connections to block known attacks	EAL4
SR 10: Use secure application software configurations	EAL5
SR 10a: Maintain Security patches for application software	EAL5
SR 11: Data must be securely encrypted before uploading	EAL5
SR 12: Each log in by user agent must be logged.	EAL4
SR 13: The asset (inventory) must be regularly checked for unauthorized changes	EAL5

DIACAP Activities

DIACAP is a comprehensive documentation of all aspects of the C&A process. It does the following:

- Describes the operating environment and threat
- Describes the system security architecture
- Establishes the C&A boundary of the system to be accredited
- Documents all requirements necessary for accreditation
- Minimizes documentation requirements by consolidating applicable information (security policy, concept of operations, architecture description, test procedures, etc.)
- Documents the DIACAP plan
- Documents test plans and procedures, certification results and residual risk
- Forms the baseline security configuration document



Based on the DIACAP activities, we have classified some of the tasks required for MS-SIS into which category it falls and why:

Task	Activity	Why?
Risk analysis for possible attacks on MS-SIS through the internet	Initiate and Plan	This fits into the initiate and plan phase since, we need to know what could be the possible risk factors for the system. Before we can do C&A, we need to be able to identify what are the risks associated with each threat agent, plan how we can mitigate from exposing our vulnerabilities to third party agents. Before we can do C&A, we need to have this done in the initiating and planning phase so that we can decide what needs to be done. Based on the risk analysis and assessment, then, we can check the system for C&A accordingly.
Assessment of the security of system access technology used for both the external and internal users	Maintain Authorization to Operate and Conduct Reviews	The assessment should be done once the certification determination and accreditation decision is made. Once, everything is finalized then only we can assess the system before we can decommission it.
Physical Security of the MS-SIS server room.	Implement and Validate	In the implementation and validation phase, we need to check that the MS-SIS server room is physically safe. This phase includes conducting of validation activities and executing the implementation plan, and fits perfectly in this activity.

Software security testing processes for custom software developed in-house	Implement and Validate	This process also falls under implement and validate phase since, we this activity includes conducting validation activities. Since, security testing is also a form of validation to make sure that the system works properly, this falls under this activity.
Security assessment of the system management processes	Maintain Authorization to Operate and Conduct Reviews	Once, we have made the certification determination and accreditation decision, then we can do an assessment of the system management processes and hence, falls under this activity. This activity includes conducting review, and assessment is a type of review.

BCDR - Business Continuity / Disaster Recovery Plan

Incident Response Plan (IRP)

IRP is required for the immediate response to an incident. In many cases, IRP is sufficient to restore the systems and when there is a major IT outage, the DRP is made operational.

Notification of key personnel	The personnel on the incident response team should be notified who should be available 24/7. This could be done on a rotation basis. If it is an attack then, the security officer should upon determining that is an attack should contact the CISO.
Analysis	Once we check what kind of attack it is, an analysis should be done by the IT Security Team. First, we need to check if it is a known or an anticipated attack. If this attack is already there or an anticipated attack, then we should follow the protocol written on it. Then, the logs should be analyzed to see what kind of attack it is. If it is an attack, then the CISO should be notified and wait for his instructions for the protocol to follow. SEIM Alert will help notify the in-charge person and we should look at the documented process to see what is that needs to be done and if it needs to be escalated.
Containment	Once we determine that it is an attack, we need to solve this issue or prevent this from happening if a file transfer is in progress but isn't 100% complete yet. We need to halt the process, disconnect affected hosts from network and disable compromised user accounts. The containment procedures should be listed in the policies and if needed, critical functions need to be shut down. If the attack is unknown one, then steps should be documented and written what was done to contain the incident.
Evidence collection	At every point since the discovery of the attack, all kinds of evidence should be documented. If possible memory state, network logs, disk images etc. should be evidenced. Also, we need to evidence all events to CD-R to ensure it is not changed and disconnect affected hosts, and make a disk image of the hard drive without powering up the system. Also, the chain of custody should be documented.

	In the IRP, all evidence should be documented and if possible CC-TV footages, any possible logs should be kept securely. If we need to notify the regulatory authorities, we need to do that as well specially if sensitive patient information is compromised then, HIPAA and other laws might be violated.
Damage Assessment	Then, we need to do a review of the system to see what, all has been affected. An extensive network forensic testing should be done to make sure that all the system is reliable. The log must be thoroughly reviewed. All of this should be documented. If an existing procedure already exists, need to follow that. If not, then each step taken to assess the damage must be documented.
Eradication	Once, we know the damage it has caused, we need to check the Eradication procedure to make sure that all the attacks are eradicated. Need to remove all possible Trojans, worms, rootkits, bots etc. If the attack is a new one, all possible things done should be documented.
Recovery	Once, the system is clean, we need to reboot hosts, routers, restart network connections, restore files from backup, applications etc. We need to enforce a system wide password resets, ensure patching is up to date, increase logging and alerts to detect similar attacks. Everything done should again be documented.
Review and report	If any of the applicable laws such as HIPAA, or any health care laws or any law is violated then, the appropriate agency needs to be notified. Also, a report should be submitted to the management once the event is over.

Disaster Recovery Plan & BCP

In any organization, we need to have policies and procedures in place in case there is a disaster. When we have this in place, we know that we are prepared for any kind of incidents that may affect our business. DRP refers to actions needed to be taken in case there is a natural disaster which affects the operation of the system or a severe damage to our servers because of which our system becomes inoperable. In either of these cases, we need to be prepared and make sure that we have controls in place to combat such issues in the case of a disaster.

The purpose of this Backup & Restore, Business Continuity / Disaster Recovery Plan is to enable the sustained execution of mission critical processes, mainly remittance processing system, in the event of an extraordinary event that causes this system to fail minimum production requirements.

The contingency plan will assess the needs and requirements so that it may be prepared to respond to the event in order to efficiently regain operation of the systems that are made inoperable from the event.

Marvel's Backup & Restore, Business Continuity / Disaster Recovery process is handled by software service providers as part of the software lease term. All servers are configured with RAID mirroring in case of any hard drive failure.

Backup & Restore

MSIS Server: The primary business critical server hosted with *SoftLayer* hosting provider. The business-critical system is being backed up twice a day. A *full backup* of the system occurs *every night* and a *differential backup* occurs every *mid-day*. These backups happen in *SoftLayer* hosted *solutions provider* at their Washington, DC facility, then it gets replicated in real-time to another mirrored *offsite* server hosted with ShinJiru Data Center*,* an IT infrastructure hosting company based in Malaysia and Singapore.

The retention on these backup sets is one month. In case of data lose or delete happens, a verbal and email request to be sent to the IT team for restoration. Standard time for restoration of a file is one to two hours.

Business Continuity / Disaster Recovery Plan

Definition of a Disaster

Elective

A disaster can be caused by man or nature and results in Marvel's IT department not being able to perform all or some of their regular roles and responsibilities for a period of time. Marvel defines disasters as the following:

- One or more vital systems are non-functional
- The building is not available for an extended period of time, but all systems are functional within it
- The building is available, but all systems are non-functional
- The building and all systems are non-functional
- The following events can result in a disaster, requiring this Disaster Recovery document to be activated:
- Edit this list to reflect your organization
- Fire
- Flash flood
- Pandemic
- Power Outage
- War
- Theft
- Terrorist Attack

Purpose - *Mandatory*

The purpose of this DISASTER RECOVERY PLAN document is twofold: first to capture all of the information relevant to the enterprise's ability to withstand a disaster, and second to document the steps that the enterprise will follow if a disaster occurs.

Note that in the event of a disaster the first priority of Marvel is to prevent the loss of life. Before any secondary measures are undertaken, Marvel will ensure that all employees, and any other individuals on Marvel's premises, are safe and secure.

After all individuals have been brought to safety, the next goal of Marvel will be to enact the steps outlined in this DISASTER RECOVERY PLAN to bring all of the organization's groups and departments back to business-as-usual as quickly as possible. This includes:

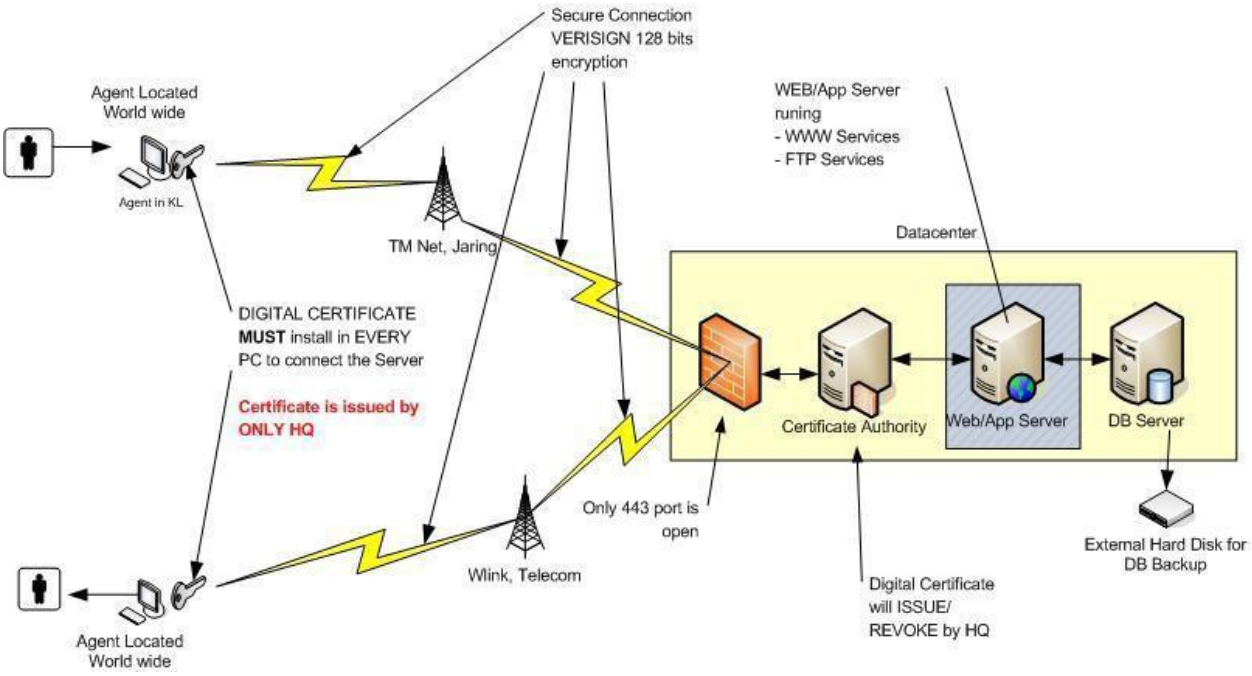
- Preventing the loss of the organization's resources such as hardware, data and physical IT assets
- Minimizing downtime related to IT
- Keeping the business running in the event of a disaster

Scope - *Mandatory*

The Marvel DISASTER RECOVERY PLAN takes all of the following areas into consideration:

- Network Infrastructure
- Servers Infrastructure
- Telephony System
- Data Storage and Backup Systems
- Data Output Devices
- End-user Computers
- Organizational Software Systems
- Database Systems
- IT Documentation

MS-SIS System: The primary business critical server hosted with *SoftLayer* hosting provider at their Washington, DC location. There is another mirror server hosted at *ShinJiru Data Center,* an IT infrastructure hosting company based in Malaysia and Singapore. These two servers replicate data to each other in real-time and they are set as active and passive mode. In the event of connection lose and disaster in primary hosting site, IT team will manually d make the secondary server hosted with ShinJiru as the active server. This process should take no more than 10 minutes as tested. Below is the layout of the infrastructure:



Strategy Roadmap

This section will define strategic initiatives for company to execute over a span of three years based on identified priorities

When Marvel IT was building a strategy, there have been ambitious plans for next 3 years.

- International Expansion in 10 Countries by 2020

  The goal is to expand in the international market, that's always been the vision of the Marvel Studios to tap into the international film industry. By enabling this platform, it will help us engage the global scale of the industry.

- Migrate 80-90% IT Infrastructure to Cloud by 2020

  Marvel Studios is a media & entertainment company, we don't want to invest a lot of our budget every year on procuring and maintaining the new hardware. We are open minded company and willing to take challenges. Marvel Studios want to focus primarily on the media & entertainment business, least to care about the IT enablement services.

  Thus, the goal will be to migrate as much workloads as possible to the cloud based model by 2020.

- Monitor, Prevent & Detect new & existing Threats
  E.g. Ransomware - What if celebrity database gets attacked??
  Reference: https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

  Just-In Time Access – MS-SIS Infrastructure
  Just-Enough Access – MS-SIS Infrastructure

  It's not just about building a great solution and let it run in a box in the corner. Marvel IT have envisioned a rock-solid security design to make sure that we protect customer data at any cost and all the time. Marvel IT Teams is always open to evaluate the new security enhancement built to enforce the platform security.

- Next-Gen Development Platform for MS-SIS
  E.g. Containers, BlockChain, HoloLense, .NET STD

  As a part of the strategy roadmap, the most important of all is to leverage all the new technologies such as BlockChain, Containers, Mixed Mode Reality, Cross-Platform Development to make sure in the coming years we are up to the speed for all the major platform available in the market.

Conclusion

Marvel IT is ambitious about Marvel Studios – Secure Image Solution (MS-SIS) platform. It's being developed with the employees like photographers, editors in the mind. The MS-SIS Solution is built using modern state of the art technologies, making the code-base and the solution robust for upcoming years.

As it's designed using the modern platform and deployed public cloud, the fundamental strategy and goal was to make sure that the platform is robust and can adapt the new technologies and changes effectively.

As you can see we have been spending a significant amount of time on building the MS-SIS Platform for Marvel Studio.

In the coming months, we will be working with different teams within the Marvel Studio Teams to work on the onboarding of the MS-SIS Solution so that all the teams within the Marvel Studios can leverage and engage with the MS-SIS Platform on day to day basis.

As building this document is a commitment of the Marvel Studios IT Team to demonstrate that we do have a solid plan meet our GO LIVE date to finish the MS-SIS Platform Project as a great success.

References

Goals, Guiding Principles
https://www.helpnetsecurity.com/2009/10/20/7-guiding-principles-for-redefining-information-security/
http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf
http://phibetaiota.net/2009/10/journal-information-security-seven-guiding-principles/
http://phibetaiota.net/2009/10/journal-information-security-seven-guiding-principles/
https://www.welivesecurity.com/2016/05/24/critical-infrastructure-time-make-security-priority/
http://electronicdesign.com/iot/end-end-iot-security-starts-infrastructure
https://www.thingworx.com/blog/6-approaches-to-developing-iot-solutions-more-efficiently/
https://www.forbes.com/sites/kalevleetaru/2017/03/20/recapping-google-next-17-making-security-seamless/#33b6174dc4e8
https://www.winmagic.com/resource-centre/white-papers/five-pillars-of-transparent-data-security
https://digitalguardian.com/resources/data-security-knowledge-base/content-aware-security
https://daniel-rs.github.io/files/publications/noms2014_paper.pdf
https://www.ciscolive.com/online/connect/sessionDetail.ww?SESSION_ID=90059&backBtn=true

Management of the Deployed System

ISO/IEC 17799:2005
Azure Security Incident Response
Microsoft Azure Compliance
Chapter 6: Information Systems Security
Azure Active Directory – Role-Based Access Control (RBAC)
Azure Active Directory – Role-Based Access Control (RBAC) Configuration
Microsoft Azure – Security Center