IST 654

Root Cause Analysis for HCG

(Describing the Root Cause for HCG using Fishbone and 5 Why Analysis)

BY:

Name: Saurabh Jape

Team Name: ANALYZERS

Team Number: 05

Mentor: Vishakh Viswanathan

Meeting Time: Tuesday (8pm-9pm)

Meeting Venue: Hinds Hall – Room 216

Table of Contents

HEALTH CARE GROUP – *A Brief Overview*

The Health Care group has been seriously affected by a data breach. They are unable to trace the source of the breach. Security is a major requirement in any organization and data breach is a very serious problem that any organization can face. It is important to take immediate action to ensure that data breaches do not occur in future.

Taking action to secure data is extremely important in todays world. Fines of up to around $500,000 can be imposed by the Information Commissioner on organizations that do not comply to the data protection compliance. Apart from this, individual/customer's can claim severance payments against the organization that have been affected by the data breach. This has a fatal impact on the organization. Organizations incur high costs of disruption to investigate and respond to the incident and such incidents damages the reputation of the business's brand and reputation.

Responding to a breach:
It is thus highly important for an organization to take prompt action to investigate and contain the incident. Steps should be taken to assess whether the data can be recovered and minimize the damage associated with the breach. This involves analyzing the possible reasons for the breach and performing a root cause analysis to ensure such situations do not arise in future.

Current Process:
Currently, the Health Care group work manually in making and filing claims. The process of out of pocket expense calculation, claim processing and re-pricing, claim notification, finance and auditing process and the entire system contain various points where manual updating and calculation takes place. These are areas where data breach could be highly possible.

The systems used could have become vulnerable and obsolete. There could be malicious intent by people, environmental aspects, compliance related regulation failures, system failures, lack of effective processes and policies etc. which are all possible reasons for the security breach. There could be many other such reasons that results in a data breach, hence analyzing all aspects of the system is extremely important.

The focus of this document is to identify various possible reasons that could have led to the data breach, thereby deducing the root cause of the data breach problem. The fishbone diagram helps identify various possible reasons i.e. the symptoms of the data breach. This is followed by the 5 why analysis that helps dig deeper into each symptom and reach the root cause. Finally, the resolution table helps resolve the root cause using BPR, IT System or Risk Mitigation thereby helping understand and eliminate the data breach issue.

Cause-Effect Analysis

The Health Care group has been seriously affected by a data breach. They are unable to trace the source of the breach. It is important to trace the source of the breach.
The effect in the problem statement that is being analyzed is- **Data Breach**

The symptoms can be classified under the following categories:

1) System:
   a) Lack of Security present in the system
   b) Unauthorized Access to users
   c) Lack of auditing of the system

2) People:
   a) Mistakes and Manual Errors by the system users
   b) Lack of awareness and training provided to the employee
   c) Protection against physical theft of devices awareness
   d) Lack of ethics amongst employee

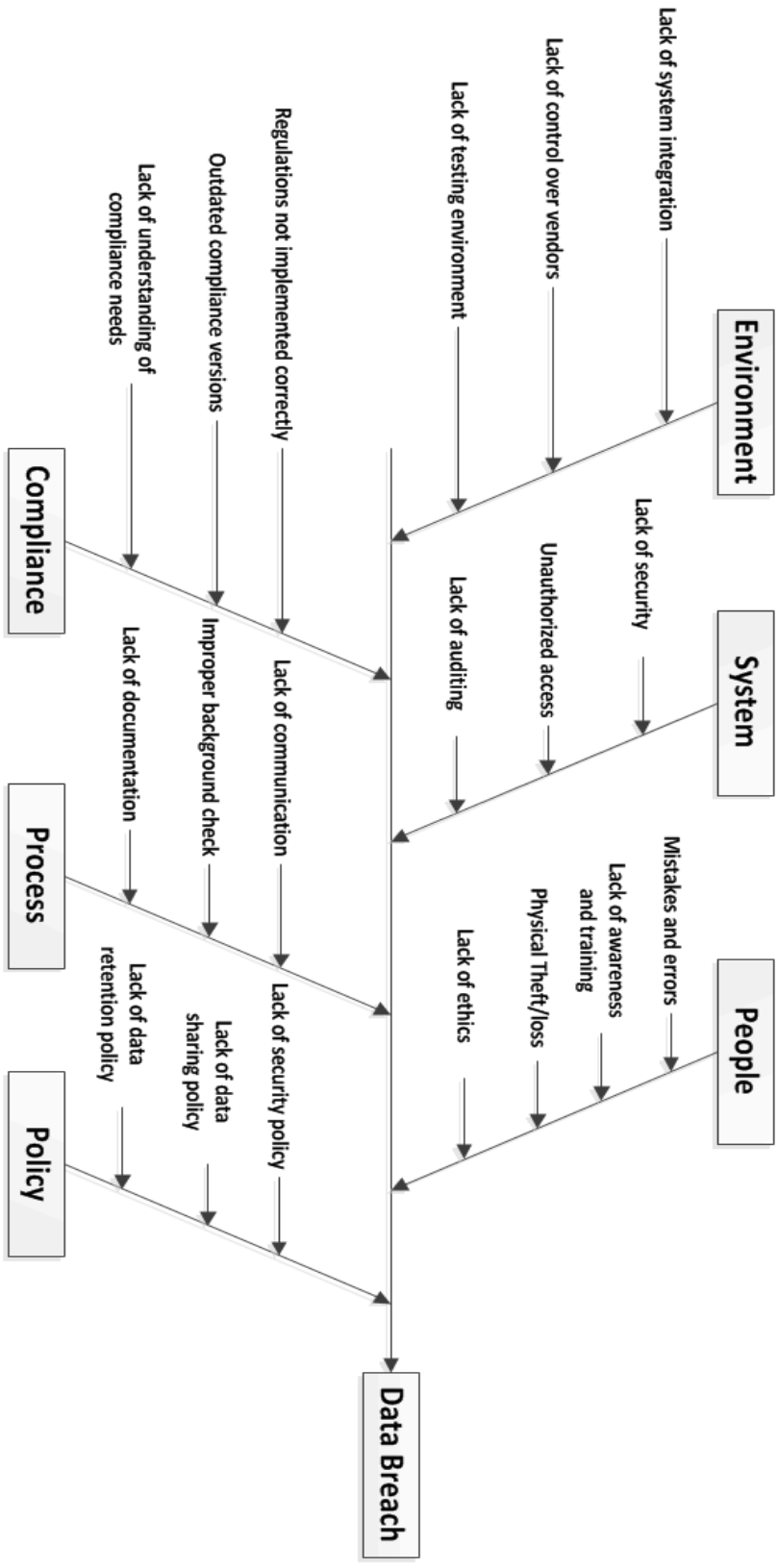
3) Environment:
   a) Lack of system Integration
   b) Lack of control over vendors
   c) Lack of testing environment

4) Process:
   a) Lack of communication to the lowest level in the organization
   b) Improper process of background checks of employee
   c) Lack of documentation process

5) Compliance:
   a) Regulations not implemented correctly
   b) Outdated compliance version
   c) Lack of understanding of compliance needs

6) Policy
   a) Lack of security policy
   b) Lack of Data Sharing policy
   c) Lack of Data retention policy

FISHBONE DIAGRAM:



ROOT CAUSE ANALYSIS – *5 Why Technique*:

CATEGORY	SYMPTOM	5 Why's ?
1. PEOPLE	**Mistakes And Manual Errors**	• **Why are there mistakes and manual errors?** Manual errors are caused due to the typing/writing errors by the staff while entering user and claim details. • **Why are typing errors caused?** These are caused due to employee fatigue. • **Why are employees getting tired?** The employees are working overtime that is causing fatigue. • **Why are the employees working overtime?** The employees are working overtime as they have to manually work on the user details and claim processing. • **Why are the employees working manually?** The employees are working manually because there are no existing IT systems. **Root Cause: There is no existing automated IT system which can replace the existing manual system.**
	Lack of Awareness	• **Why is there lack of awareness amongst the employees?** No sufficient training and information provided to the employees on the use of systems. • **Why is there lack of training and information provided to the employees?** There are very few experts that can provide training compared to the size of the employees that require training. • **Why are there very few experts to train the employees?** The organization feels that the number of current experts are enough to train the employees. • **Why does the organization feel that the number of experts are enough?** The company spends less on hiring experts and tend to over work the experts. • **Why are the experts overworked?** The company has a faulty recruiting policy. **Root Cause: Fault in the recruiting policy as they neglect hiring experts.**

	Physical Theft and loss	• **Why is there theft and loss?** Employees are not serious about the protection of assets that contain secure data. • **Why are employees not that serious about device protection?** Employees take the security of devices for granted and do not take enough precautions. • **Why do the employees not take enough precautions?** The employees are not aware of the steps that they should take in case of theft and the consequences that theft or loss of devices can have. • **Why are the employees not aware of the steps and consequences of theft/loss?** There is no flow of information to the lowest level of the organization. • **Why does information not flow to the lowest level of the organization?** There are no knowledge sessions that take place in the organization, such as seminars and trainings. **Root Cause: Lack of training, information sessions and webinars on the need and steps to ensure security.**
	Lack of ethics	• **Why is there a lack of ethics amongst the employees?** Employees are not serious about the work that they do and the culture. • **Why are employees not that serious about their work?** Employees feel that they are underpaid with respect to the amount of work that they do and their work is not recognized. • **Why do the employees feel that they are underpaid and their work is not recognized?** The employee's salaries have not increased, there are no promotions. • **Why are the employee's salaries not increased?** The organization very rarely announces bonuses and promotions. • **Why does the organization not announce bonus?** The organization does not focus enough on employee incentives and recognition for employees. **Root Cause: Lack of focus on employee incentives, promotions and bonuses.**

2. SYSTEM	**Unauthorized access**	• **Why does the system allow unauthorized access?** The system provides access to partners, hospitals as admin users. • **Why does the system provide access to partners, hospitals as admin users?** The system was designed to provide access to partners, hospitals so that they can update the patient health details and claim details and view the status of the claim that is being processed. • **Why can partners, hospitals update the patient health details and claim details?** The partners and hospitals can update the patient health details to monitor the health of the patient and update the ICD codes manually in case of conversion failure. This can be done easily post registration. • **Why are partners and hospitals able to register easily?** The system allows a user to register as a partner or hospital easily. There is no background verification/ check performed by the system to verify the authencity of the user. • **Why is there no background verification?** The system designed was poor and has not been updated. **Root Cause: Poor IT system design due to which there is no background check in place.**
	Lack of security	• **Why is the system unsecure?** The system is unsecure because it is unable to respond to the viruses, hacks and web attacks. • **Why is the system unable to respond to the viruses, hacks and web attacks?** The viruses, hacks and web attacks have increased and systems are unable to respond because they are slow and are unable to detect. • **Why is the system slow and unable to detect viruses, hacks and web attacks?** The system uses a security mechanism that is inefficient against todays attacks. • **Why is the system inefficient to todays attacks?** The system uses a security mechanism that is outdated • **Why does the system use outdated security tools?** The system was built a long time ago and has not been updated. **Root Cause: The system security tools have not been updated and are outdated.**

	Lack of auditing	• **Why is there a lack of auditing?** The system worked well and therefore importance was not given on auditing. • **Why was low importance given to auditing?** The process of auditing is extremely complex and has various aspects to it. • **Why is the auditing process complex?** The auditing procedure is costly. • **Why is the auditing process costly?** The procedure requires a lot of people and time. • **Why does the procedure require many employees and time?** Auditing requires trained and skilled employees. The current skill set of employees that are involved in auditing are not at the desired standards and there are very few employees involved in auditing. **Root Cause: Lack of auditing skill set.**
3. ENVIRONMENT	**Lack of System Integration**	• **Why is there a lack of system integration?** There is lack of system integration because it is a very complex process. • **Why is it a very complex process?** System integration involves various teams coming together to integrate various parts of the system and all the teams are not in sync. • **Why are all the teams not in sync?** The teams are not in sync because each team completes their software development lifecycle at different points of time. • **Why do teams complete their development at different points of time?** Every IT team follows a different release lifecycle. This results in every team completing their projects at different points of time. • **Why do IT team follow different release lifecycle?** There is lack of planning on the date of deliverables. **Root Cause: Ineffective planning on the timelines and release dates associated with every project.**
	Lack of control over vendors	• **Why is there a lack of control over vendors?** There is lack of control over vendors because there is a lack of coordination. • **Why is there a lack of coordination?** There is a lack in coordination as various vendors change the details associated with a claim without informing the claims admin about the change.

		• **Why do vendors change the details without proper communication?** The vendors have complete access to the portal, thereby allowing them to update and modify the details easily. • **Why do vendors change the details easily?** The changes get reflected without anyone validating the changes. • **Why doesn't anyone validate the changes?** The system is designed in such a way that the vendor's changes do not have to be validated. **Root Cause: Poor system design. No validation in place to validate the vendor changes.**
	Lack of testing	• **Why is there a lack of testing?** There is lack of testing because there is no environment available for testing to be completed on time. • **Why is there no environment available for testing?** All the environments that are present are being used for deploying productions code of previous quarter. There is no environment that has been setup for the next release cycle. • **Why has the environment not been setup for the next release?** The environment could not be setup for the next release as there is no server configuration that has been purchased by the organization. • **Why has the organization not purchased a new server configuration?** The IT team did not buy new servers as they were going to use the existing servers. They failed to consider the fact that the previous servers would be used as the production sample server. • **Why did the IT team not consider the existing server problem?** There was lack of planning by the IT team. **Root Cause: Lack of planning by the IT team on the ordering of server stack.**
4. COMPLIANCE	**Incorrect implementation of regulations**	• **Why is there an incorrect implementation of regulation?** The system has implemented incorrect security constraints because of incorrect understanding of the requirement.

		• **Why was there an incorrect understanding?** The requirements that were developed by the developer of the system were incorrect. • **Why was the requirement developed incorrectly?** The developer received incorrect instructions as there was no clarity from the higher management. • **Why was there no clarity at the end of the higher management?** The role that the higher management tried to perform was that of a business analyst. They were not experts in that area • **Why did they perform the role of the BA?** There was no business analyst in the team during the development of the system. **Root Cause: No business analyst position.**
	Lack of understanding of compliance	• **Why is there a lack of understanding of compliance?** The system developed complies partially with the security requirements. • **Why does the system only comply partially and not fully?** The system compliance was not communicated with the developers during the development of the system. • **Why were system compliance requirements not communicated with the developers of the system?** There was a feeling that communication about the compliance requirements would not be necessary. • **Why was there a feeling that communication would not be necessary?** The business thought that the system being developed would incorporate the requirements by default. • **Why did they think that the system would incorporate the functionality by default?** The business had an incorrect perception of the system that was not verified. **Root Cause: Business perception that the current system developed had the requirement.**
	Outdated compliance	• **Why are the compliances delivered outdated?** The system implemented incorrect security constraints because of incorrect understanding of the security requirement of the system. • **Why was there an incorrect understanding?** The requirements that were developed by the developer of the system were incorrect.

		• **Why was the requirement developed incorrectly?** The developer received incorrect instructions as there was no clarity from the higher management. • **Why was there no clarity at the end of the higher management?** The role that the higher management tried to perform was that of a business analyst. They were not experts in that area. • **Why did they perform the role of the BA?** There was no business analyst in the team during the development of the system. **Root Cause: No business analyst.**
5. PROCESS	**Lack of communication**	• **Why is there a lack of communication?** There is a lack of communication because there is a lack of understanding on whom to approach to. • **Why is there a lack in understanding whom to approach to?** The organization hierarchy is not clear making it difficult for employees. • **Why is the hierarchy/structure not clear enough?** There are multiple roles that an employee performs making it difficult to know whom to approach. **Root Cause: Hierarchy structure is not clear that leads to confusion.**
	Lack of documentation	• **Why is there a lack of documentation?** There is a lack of documentation because employees are forced to spend time on delivering the product instead of wasting time on documentation. • **Why are employees spending less time on documentation?** The employees have been instructed by the senior levels to spend less time on documentation. • **Why is senior leadership instructing their juniors to spend less time on documentation?** They believe that documentation takes a lot of time and is unnecessary. • **Why do they feel that documentation is unnecessary?** The senior leadership believes documentation is not productive and is less important than actually delivering work.

		• **Why do they feel that documentation is not productive?** They did not plan or analyze the actual situation. **Root Cause: The organization has an ineffective planning process.**
	Improper background check	• **Why is there no proper background check process?** There is no proper background check process because it is a very complicated process. • **Why is it a very complicated process?** Background check is a very lengthy processes that need to be followed. • **Why is the process lengthy?** The process is lengthy because it requires many resources and updated IT systems that the organization cannot afford. • **Why does the process require many resources?** The process is difficult and requires employees to perform multiple roles. • **Why are employees performing multiple roles?** The employees are overloaded and made to perform different roles for the same amount of salary as the company is working on a tight budget. **Root Cause: Tight budget that the organization is operating under.**
6. POLICY	**Lack of effective data sharing policy**	• **Why is there lack of effective data sharing policy?** Employees are not adhering to the data sharing policy. • **Why are employees not adhering to the process?** Employees are not aware of the risks associated with the file/data sharing. • **Why are employees not aware of the risks associated with data sharing?** The organization have policies in place but these are not being communicated effectively to the employees. • **Why is the communication to employees not effective enough?** The organization does not have a mechanism to ensure that the information communicated to the employees is understood by them.

		Root Cause: No proper communication channel to ensure that data sharing policy is understood by the employee.
	Lack of security policy	• **Why is there a lack of security policy?** Due to incomplete understanding of security risks associated with a business. • **Why is there incomplete understanding of security risks?** There is no skilled expert who knows about the importance of security policy implementation. • **Why is there no skilled expert for ensuring security policy?** The organization has not hired skilled experts for ensuring security policy. • **Why has the organization not hired anyone to ensure security policy?** The organization leadership was not aware of the importance of secure policies and the risks associated. • **Why was the organization not aware of the importance of security policy?** The organization did not focus on security policy during the initial stages. **Root Cause: Lack of focus on the importance of security policy and the risks.**
	Lack of effective data retention policy	• **Why is there lack of effective data retention policy?** Employees are not adhering to the data retention policy. • **Why are employees not adhering to the policy?** Employees are not aware of the risks associated without data retention. • **Why are employees not aware of the risks associated without data retention?** The organization have policies in place but these are not being communicated effectively to the employees. • **Why is the communication to employees not effective enough?** The organization does not have a mechanism to ensure that the information communicated to the employees is understood by them. **Root Cause: No proper communication channel to ensure that data retention policy is understood by the employee.**

Resolution Table:

The Major root causes identified from the 5 Why Technique are:

1. **No existing automated IT system which can replace the existing manual system**
   - Mistakes and Manual Errors
2. **Fault in the recruiting policy as they neglect hiring experts**
   - Lack of awareness
   - Incorrect implementation of regulations
   - Outdated compliance
3. **Lack of focus to ensure security**
   - Physical theft and loss
   - Lack of security policy
4. **Lack of focus on employee incentives, promotions and bonuses**
   - Lack of ethics
5. **Outdated system security tools**
   - Lack of security
6. **Lack of effective skill set**
   - Lack of auditing
7. **Ineffective planning**
   - Lack of testing
   - Lack of System Integration
   - Lack of documentation
8. **Poor IT system design**
   - Lack of control over vendors
   - Unauthorized access
9. **Business perception**
   - Lack of understanding of compliance
10. **Tight budget and limited funds**
    - Improper background check
11. **Ineffective communication channel**
    - Lack of effective data sharing policy
    - Lack of effective data retention policy
12. **Hierarchy structure is not clear**
    - Lack of communication

The 3 resolution techniques considered for the resolution table are:

- BPR : BUSINESS PROCESS REENGINEERING
- IT SYSTEM : CREATING AN IT SYSTEM
- RISK MITIGATION : MITIGATING THE RISK ASSOCIATED

Root Cause	Symptom (Causes)	BPR	IT Engineering	Risk Mitigation
1. No existing automated IT system which can replace the existing manual system	Mistakes and Manual Errors	The employees work load shall reduce, which does not lead to fatigue, thereby reducing manual errors. Each employee shall work only for a maximum of 8 hours.	The IT system will have validation checks to ensure verification of the details like name, date of birth, claim submitted date, claim submitted by etc. that are entered by the user. The manual processing of claims and enrollment management would be taken care by the IT system.	**Risk:** The user can still enter incorrect details. **Mitigation:** The changes made would be sent to a senior employee for approval.
2. Fault in the recruiting policy as they neglect hiring experts	Lack of awareness	The organization shall spend more on hiring skilled and high quality experts that will help create awareness throughout the firm.	Web based trainings would be introduced in the internal system for employees to ensure awareness amongst employees coupled with interactive quizzes	**Risk**: The organization might not be able to recruit many experts. **Mitigation**: The experts recruited would lead a team and conduct training sessions for them. The team would then train other employees.

	Incorrect implementation of regulations	The organization shall focus on hiring skilled and high quality experts that are aware of the regulations and its implementation.	The systems would be revamped according to the inputs received from the experts to make sure that the regulations are met. This would require system analysis to ensure that the changes suggested are compatible.	**Risk**: The organization might have to update the systems that would involve high costs. **Mitigation**: The update of systems and process revamp would ensure meeting regulation guidelines.
	Outdated compliance	The organization shall focus on hiring skilled experts that are aware of the latest compliances that are out there in the market and its implementation.	The systems would be revamped according to the inputs received from the experts to make sure that the compliances are met. This would require system analysis to ensure that the changes suggested are compatible.	**Risk**: The organization might have to update the systems that would involve high costs. **Mitigation**: The update of systems and process revamp would ensure savings on compliance penalties.
3. Lack of focus to ensure security	Physical theft and loss	The organization shall focus on improving the employee awareness and the need of security through training and seminars. The training shall be mandatory and each employee would have to attend the training.	The internal systems would add Web based trainings to ensure awareness amongst employees. The employees would login to the system, register for webinars, seminars and training sessions. The system would record each employee activity and produce a list of defaulters.	**Risk**: The employees might skip the sessions and not attend the web based trainings. **Mitigation**: The employees would be made to give interactive quizzes which would have an impact on their appraisals.

	Lack of security policy	The organization shall focus on improving the security policies within the organization by restructuring the security policies in accordance with the latest security policies. This would be done by conducing a meeting between the respective required members to analyze the differences and the gaps that need to be filled.	The updated security policy decisions would be communicated to each employee of the organization through the internal system portal and outlook so that employees are informed about the recent changes in security policy.	**Risk:** The security policy may become obsolete in the near future. **Mitigation:** The security policies would be monitored on a quarterly basis to ensure that the policies are up to date. Meetings would be conducted on a regular basis to analyze the position and come up with the solutions.
4. Lack of focus on employee incentives, promotions and bonuses	Lack of Ethics	The organization shall focus on improving the rewards, recognition, incentives and promotion.	The system shall be updated with a tool to log in hours, daily effort and the supervisor's comments to increase transparency and to awards certificates and honors to the hard working employees.	**Risk:** The increased competition could result in quarrels and fights amongst employees. **Mitigation:** The system would be transparent and individuals would have the option to notify the supervisor or the HR incase of any dispute.
5. Outdated system security tools	Lack of security	The organization shall perform a thorough analysis and come up with a list of outdated security tools.	The system would be updated with the latest technology to counter the various problems associated with security. The gaps present in the current system would be filled.	**Risk:** The security tools may become obsolete in the near future to protect against future attacks. **Mitigation:** The security tools would be monitored over a regular period of time and the

				performance would be measured.
6. Lack of effective skill set	Lack of auditing	The organization shall improve the process to increase the quality of auditing by recruiting additional personnel or by training current auditors through training sessions.		**Risk:** One-time auditing would have a risk of further issues coming up in future. **Mitigation:** The auditing would be required over a monthly basis to ensure the smooth and secure functioning of the system.
7. Ineffective planning	Lack of testing	The organization shall improve the process of planning to ensure that servers are bought way in advance so that there is a testing environment in place. The process improvement would include analyzing potential areas of improvement.	The system would be updated to notify the users about which environment is used up and which ones are free to use.	**Risk:** Buying servers year after year would be costly. **Mitigation:** Two sets of server pairs would be bought and reused each qtr.
	Lack of System Integration	The organization would improve the process of planning project release dates to ensure that projects lifecycles are similar so that integration would become easier and in sync.	N/A	**Risk:** Project teams would need to wait for the one another to finish, thereby increasing the waiting time. **Mitigation:** Every project would be spread over phases such as- development, testing, pre production and go live to ensure that

				each project is in sync throughout the lifecycle.
	Lack of documentation	The organization shall spend more time on analyzing and documenting the requirements. Documentation shall be handled by each employee for their own functionality.	The system developed would be tested in accordance to the documentation to ensure all security constraints are in place in the system built. The documents would also be stored securely.	**Risk:** Documentation would increase a lot of material that would become difficult to handle. **Mitigation:** The documents shall be maintained in a central repository in a date-wise manner to ensure all the information is preserved with access only to admin users.
8. Poor IT system design	Lack of control over vendors	N/A	The updated system shall contain a validation UI for the admin users to view and approve the changes made by the vendors. All changes made would be logged by the system.	**Risk:** Admin users would be given rights to control the entire system. **Mitigation:** Admins would be selected after a thorough background check to prevent corrupt and malicious intent.
	Unauthorized access	N/A	The system shall contain a mechanism to check the authorization of the user and the details entered to prevent access. Updated password mechanisms would also be put in place to ensure authorized access.	**Risk:** The authorized users could leak out data. **Mitigation:** Each user that logs into the system and their activity would be monitored to ensure protection against such acts.

9. Business perception	Lack of understanding of compliance	Effective communication channels would be setup to ensure perception is cleared out at the initial stage itself. Weekly meetings would be held to ensure complete understanding at every step.	N/A	**Risk:** There could be perceptions that would be missed during the initial stages. **Mitigation:** The perceived perceptions would all be documented and raised with the concerned person to ensure that no requirement is missed to ensure that the system security does not have loop holes.
10. Tight budget and limited funds	Improper background check	The organization shall ensure that proper budgeting is done to ensure that the employees are not overworked. This would help resolve the background check issue due to mistakes and errors due to overwork.	The system shall also contain a mechanism to check the authorization of the user and the details entered to prevent unauthorized access. Updated password mechanisms would also be put in place to ensure another layer of security.	**Risk:** The employees could take advantage and say that they are overworked even when they are not. **Mitigation:** The performance of each employee shall be captured by the system.
11. Ineffective communication channel	Lack of effective data sharing policy	The organization shall focus on improving the data sharing policies and communicating those to the employee through training and seminars.	The internal systems would add Web based trainings to ensure awareness amongst employees.	**Risk**: The employees might skip the sessions and not attend the web based trainings. **Mitigation**: The employees would be made to give interactive quizzes which would have an impact on their appraisals.

	Lack of effective data retention policy	The organization shall focus on improving the data retention policies and communicating those to the employee through training and seminars.	The internal systems would add Web based trainings to ensure awareness amongst employees.	**Risk**: The employees might skip the sessions and not attend the web based trainings. **Mitigation**: The employees would be made to give interactive quizzes which would have an impact on their appraisals.
12. Hierarchy Structure is not clear	Lack of Communication	The organization shall ensure that the information is effectively communicated till the lowest level of the organization. This would be done by organizing an effective structure that helps in the smooth flow of information. This would require revamping and defining clear roles to every employee.	The organizational internal tool would be revamped to take note of this change. This would include adding employee details, role and current project involved that would make the process transparent and clear.	**Risk:** Even after an effective structure is in place, communication problems could still arise. **Mitigation:** The system would provide employees with a feature where they can log in complains and problems that they are facing. The information gathered would be communicated to the respective authority.

CONCLUSION

Thus, the above analysis helps determine the root cause for various symptoms identified for the case. The cause-effect diagram helps analyze all the possible symptoms, the 5 Why techniques helps reach the root cause of every symptom and finally the resolution table helps to solve the root cause, thereby eliminating the problem.