**NATIONAL DNA DATABASE CASE STUDY PROJECT RISK FMEA REPORT**

**Table of Contents**

[Chapter 1: Introduction and Background 3](#_30j0zll)

[Chapter 2: Failure Mode and Effect Analysis (FMEA) 4](#_1fob9te)

[Chapter 3: Risk Response Strategies 7](#_3znysh7)

[Chapter 4: Risk monitoring and control strategy 9](#_2et92p0)

[Chapter 5: Quality and Change Control Strategy 11](#_tyjcwt)

[Chapter 6: Conclusion and Recommendations 12](#_17dp8vu)

[Reference list 14](#_26in1rg)

# **Chapter 1: Introduction and Background**

Every project irrespective of its size requires a certain amount of planning. Without resorting to a predetermined pattern it tends to get difficult to sort resources accordingly. When one considers the underlying notion concerning the development and deployment of large-scale projects, the number and frequency of potential risks and threats increase by a considerable margin. Planning fallacy has surfaced as one of the biggest shortcomings when it comes to fuelling the occurrence of project failures. The foremost cause behind the failure of a plethora of projects primarily involves the inefficiency of the management department to fathom the time, cost and implications concerning a project. More often than not organisations/facilities underestimate the strategies and engagement of the stakeholders while planning the project and suffer because of it. While taking part in large-scale projects, one of the foremost obligations involves chalking out a proper strategy, which needs to be planned in accordance with the projected outcomes and chances to encounter possible hurdles. This particular task involves analysing a set of possible risks concerning the full-scale development and implementation of a government database. The idea is to make certain that the database excels in holding all the DNA-related records of individuals from the UK.

It needs to be addressed that the DNA-related information of an individual is a piece of sensitive information and it holds the very identity of the person. If not managed properly, it might end up in the wrong hands. This would not only compromise the privacy rights of a person but it would also bring serious implications for the government as a whole. The study takes a plunge into the details concerning the development of the database and unearths some of the foremost risks concerning the project and the hurdles it might encounter during the development as well as deployment phases.

# **Chapter 2: Failure mode and Effect Analysis (FMEA)**

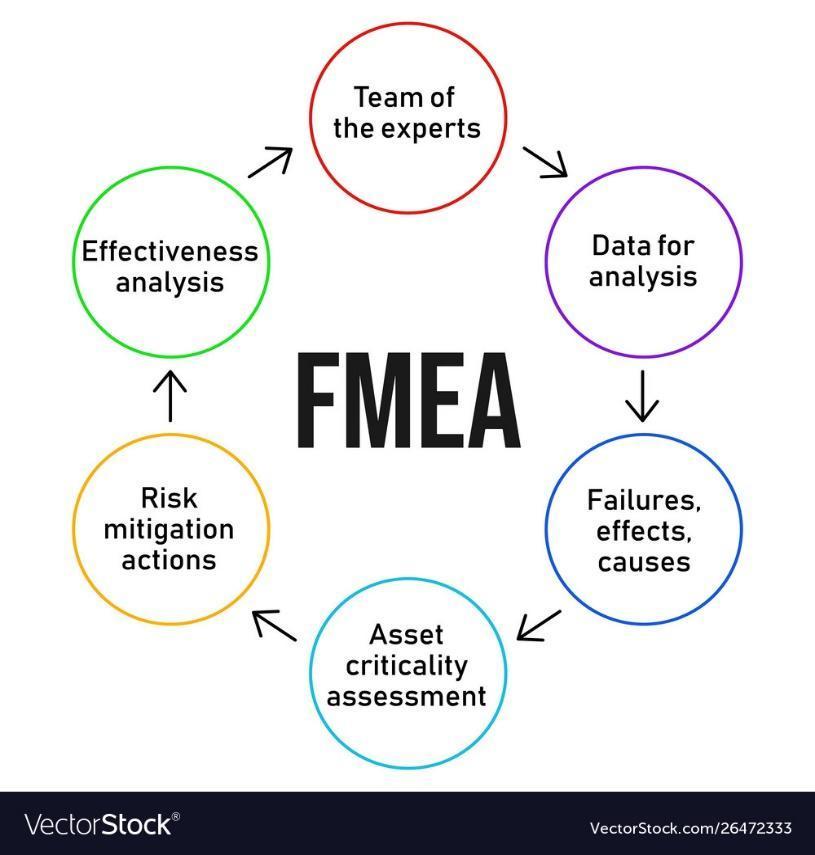


Fig: Failure mode and Effect Analysis (FMEA)

Source: (Subriadi and Najwa, 2020)

The very notion concerning the application of the Failure Mode and Effective Analysis (FMEA) deals with sorting all the possible categories of risks into multiple areas and then assigning each of the following factors; i.e. the severity (SEV), the chances of occurrence (OCC) and detection rate (DET) with a numerical value in order to derive a risk priority number for each of the identified areas (Subriadi and Najwa, 2020). The project must be performed adhering to descending progress of the risk priority values. All the mitigation strategies concerning the project must be focussed and based on the recorded risk priority numbers for all the identified factors. The following table exhibits the potential risks concerning the development of the National DNA database.

| **Risk area** | **Reasons behind potential failures** | **Implications** | **SEV (Out of 10)** | **Potential causes** | **OCC** | **Current Process controls** | **DET** | **RPN** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Integration difficulties | NHS may face challenges while integrating the DNA database | Data privacy, inconsistency in data and latency can occur in the system | 5 | Lack of skills. Lack of planning and lack of integration standards | 5 | Designing a proper integration strategy | 6 | 150 |
| Reluctance to change | The hospital system may face challenges with new systems | System failure, poor data management | 7 | Lack of knowledge, lack of awareness | 4 | Effective communication and several awareness campaigns | 5 | 140 |
| Data breaches | The occurrence of data breaches while handling this sensitive system | privacy concerns, and reliability issues | 4 | Cyber attacks, inefficiency to resort to cyber security protocols (Helo *et al.,* 2020). | 9 | Securing the database with firewalls and IDSs | 5 | 180 |

Based on the outcomes of the FME Analysis, it can be deduced that the Risk Priority Number of the ethical concern is data breaches associated with the project is the maximum, i.e. 180. All the numerical values which have been assigned rate the areas of risk on a scale of 10, with 1 implying the best condition and 10 implying the worst.

The risk areas that the report of the analysis illustrates include the concerns of data breaches, difficulties in integrating the NDNA Database with the system and reluctance to adapt to this new change.

***Data breach:*** It needs to be addressed that the study involves the association of sensitive information of a plethora of individuals, if not managed and stored properly, the information in the wrong hands can wreak serious havoc (Gerke *et al.*, 2020). The foremost factors which trigger these ethical concerns include the increased frequency of data breaches, encountering server overloads and experiencing insubordination from the developers. These factors possess the potential to bring a sudden and unexpected series of unforeseen dynamics, which might disrupt the system for good. Since the implications concerning this area are the most of all, the RPN value concerning the area is the maximum, i.e. 180.

***Reluctance to change***: through the study, it has been seen that due to a lack of awareness and knowledge patients at the hospitals may fail to cooperate with the new system which can be resulted in mismanagement of the system and not the availability of the information as per requirements. After analysing the risks factor, it seems the RPN value of this concerning factor is 140, which is also needed to be mitigated as early as possible.

***Integration difficulties:*** from the analysis of the risks in the case of NHS, it also has been seen that the hospital systems may face challenges while integrating with a new DNA database as data can be lost, and latency can occur. The RPN value for this risk is 150 which seems quite high and needs proper strategies and guidance to mitigate such challenges.

Deriving implications concerning all the areas, it can be established that the success of the project is completely based on its efficiency to uphold the ethical considerations which come with it. A part of the project management plan must highlight the significance of resorting to the application of Intrusion detection systems and a set of cyber security protocols in order to meet this very need. The predetermined budget for the project must integrate all these factors along with a contingency plan (in case breaches are encountered even after adhering to all these strategies).

# **Chapter 3: Risk response strategies**

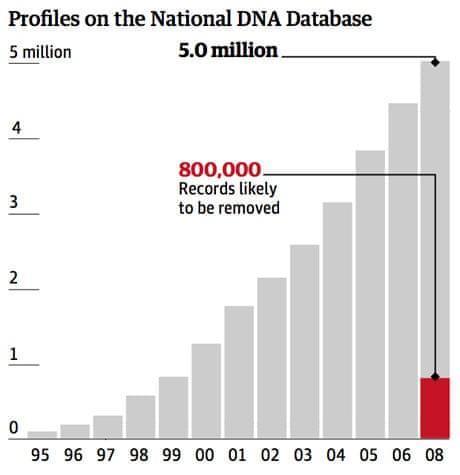
H

Fig: Profiles on the National DNA database

Source: (*The Guardian*, 2009)

(Kerman *et al.,* 2020) has concluded that there are a number of things that can affect a project event and government project also. As per the findings of (Kerman *et al.,* 2020), possible reasons can be technical failure, environmental issues, financial complications, lack of skilled professionals, ethical issues and others but these factors are based on the type of project. Based on these issues, the development of a risk response plan is associated with risk assessment, risk identification as well as response strategies of mitigation that determine the success or failure of the project. This entire project is the implementation of a DNA database in all NHS hospitals. Thus, there are a number of chances of occurring issues before starting the project and during the project.

Based on the project, the risk response plan has explained the strategies that can be considered to solve the negative effects of identified project risks (Kerman *et al.,* 2020). Three major risks have been identified in this project that can hamper the outcome of this project. Thus, it is essential to develop a risk response plan that will help to decrease or eliminate any threats to the project of implementing DNA databases in each hospital of the NHS.

The following risk response strategies will be followed to mitigate or protect the entire project from any threats.

Among identified risks, ethical consideration i.e data breach has scored much and was considered the most concerning issue within this entire project.

**Avoid**

This strategy of risk response is about avoiding particular risks as it is detrimental to the project. From the FMEA analysis, it has been identified that data breach risk has scored 180. In this entire project, difficulties may arise from technical failures or mismanagement (Chen *et al.,* 2020). As this project is managed through the UK government, in this case, the project manager is completely dependent on the Government. In this situation, the Government should avoid the risks of mismanagement by removing conflicted persons within the project. But this can be overseen that, these risk-avoiding strategies cannot be considered for this project of National DNA Database Case Study indeed. This is merely because, if this risk avoidance strategy can be applied to the found severe risks as mentioned, difficulties in implementation risks, reluctance to change risks and finally the ethical concerns; these risks cannot be avoided, instead they are to be mitigated towards the betterment of the mentioned National DNA Database Case Study project.

**Mitigate**

This approach of mitigation strategy could be quite beneficial for this project's National DNA Database Case Study as evidenced and proven by the occurred scenarios of risks. As this must be highlighted over here, the risks of integration of the database, reluctance to change risks and finally the ethical concerns (Taylor *et al.,* 2020). Here both the difficulties in implementation risks, reluctance to change risks and finally the ethical concerns can merely be mitigated depending majorly upon their respective severities and likelihoods indeed. These mitigation strategies will certainly be applied to the mentioned risks through certain pivotal factors which are mentioned as beneath:

* The risks that would be occurring at the time of implementing the NDNAD, the mitigation strategies that can be considered is to take the sensitive data that is in the system can convert it in the cloud system to make it more secure. This way the patients would also be able to interact with the healthcare professionals and their data would be secure in the cloud.
* The challenges of being reluctant to the changes in the system can be mitigated by conducting an awareness program to make them educated about the changes that should be there. Some guidelines have to be made for their better understanding. This way they would be reluctant to the changes.
* Here the ethical concerns-oriented risks will further be mitigated through the ongoing risk assessment in order to further determine the required changes over the needed period of time (Taylor *et al.,* 2020). These changes as well as risks will further be reported to the government and the board towards suitably facilitate the process of decision-making indeed.

**Transfer**

As this has already been mentioned, the occurred severe risks will merely be mitigated instead of transferred, avoided or accepted indeed. Therefore, this can be highlighted here that transferring the risks will not eradicate them, instead, they will stay and further they can also occur in the near future as well (Taylor *et al.,* 2020). As a solution this can be mentioned here, the government for this National DNA Database Case Study project can opt for adopting the hedging strategy in order to further adequately and competently protect this necessary project considering both the investments and resources required for this. But transferring the risks can make the project lame as the risks will still exist, merely the responsibility of this will shift from the government to another stakeholder which cannot be considered as a trustworthy solution for this project.

**Accept**

Here the mentioned three risks cannot be accepted as this strategy is mainly applied based on the severity of the risks. Seldom this can also be overseen that, the costs of minimising the risk are higher than the costs of the risk itself (Gerke *et al.,* 2020). As an example, the UK government here will not accept these above-mentioned concerns which can dramatically impact the National DNA Database Case Study Project. Therefore, instead of accepting the risks, the UK government will be more responsible in minimising them.

# **Chapter 4: Risk monitoring and control strategy**

When it comes to regulating the monitoring measures and control strategies concerning potential risks, the very notion deals with addressing and reacting to risk following a certain strategy. The approaches concerning the strategy can be classified into a series of chronological steps that must be followed with respect to the type of the encountered risk. The steps include identifying risks, classifying risks, checking the availability of the response system and eradicating risks. Considering the fact that the results of the FMEA illustrate ethical concerns regarding the project to be the risks of the highest order, it is necessary that the project adheres to a systematic approach in order to effectively combat cyber threats.

***Identifying the type of risks:*** It needs to be addressed that the database which will be developed, is supposed to function under the wings of the government and without properly identifying the type of mishap it is not really possible to develop a counter strategy, and this might end up compromising the entirety of the system. While the development operations are in progress the project management system must consider the deployment of visual tools and monitoring systems in order to verify whether or not the development operations are being performed in accordance with the established milestones (Macrae *et al.*, 2020). Even after the commencement of the deployment process, it is necessary to put in place a firewall and an intrusion detection system (IDS) (Ahmad *et al*., 2021). The idea is to chalk out the exact kind of threat effectively before proceeding to develop countermeasures.

***Classifying the type of the encountered risk:*** The development phase of the project involves the association of multiple stakeholders, but it needs to be addressed that risks can be encountered in any of the discussed phases, i.e. the development phase as well as the deployment phase. When one addresses the fact that these phases involve the integration of two different groups of stakeholders it would not be presumptuous to deduce that risks can be encountered from any possible area of operation.

***Checking the availability of the response system:*** Detecting the existence of threats is not enough, it also needs to be made certain that the threats are properly handled. In order to facilitate the project management approach must ensure that the development phase is well-equipped with adequate proper trained employees to be aware of the difficulties at the implementation time. As the other risk of reluctance, it has to be made sure that not only there have been conducted an awareness program but has to make sure that the patients are actually understanding the changes with the help of professionals and with proper guidance. On the other hand, once the deployment has been performed and a threat is encountered the system must address the presence of protection strategies like encryption and firewalls in order to prevent foreign cyber threats from making their way into the system.

***Eradicating the risk:*** Once a risk comes to being it needs to be made certain that it is not encountered all over again. The project management approaches need to take heed of the concept of absolute eradication. In the case of the time of development timing of the database system, the development team faces difficulties, then it has to mitigate with the help of proper guidance and development materials. If the project encounters a threat after the deployment phase the stakeholders must go to the root of the cause in order to unearth the risk agent and take necessary action in accordance with the findings. More often than not every cyber attack leaves digital footprints, which can be traced back to the owner. If the system lacks such features it must be made certain that the framework is equipped with adequate security setups to prevent something like that from again.

# **Chapter 5: Quality and Change Control Strategy**

The possible change control strategies for the three risks are demonstrated as beneath:

| **Prophesy of the Changes** | **Strategies to Control Change** | **Impact of the Strategy** |
| --- | --- | --- |
| Difficulty in integrating the NDNAD database into the system of NHS | Training and Workshops | The difficulty that can be faced in the time of integrating the database in all the healthcare systems is data privacy of the data that are related to health. Along with this, there is a difficulty that can be faced during integration which is EHR interoperability. In this case, big data challenges can be faced which would result in a repository of the data which is not a good idea for any healthcare data.  At the time of integrating the database for storing the DNA samples, it has to be taken into mind to secure the data in a proper way so that these problems would not occur and to do that, the employees would have to train in database systems properly. |
| Reluctance to adapt to the changing assessment methods by the patients' | Awareness Campaign | At the time a new database system is integrated within a community, the difficulties are not only faced by the development team or the employees. Patients are the one who has to deal with the changes in the systems. It takes time for them to understand and be reluctant to the new system.  Thus conducting an awareness campaign for the patients to understand the system in a better way would be helpful. |
| Quality and change control strategies against data breaches and system failure | Cyber Security Strategy | Privacy is a major long with key factor in national DNA database systems. Here the NDNAD should be aware of the fact that a well-executed IRP (Incident Response Plan) with installing a firewall could further be able to minimise complete data breaches and system failure (Subriadi and Najwa, 2020). In the case of security breaches at the time of implementing the system, each has a chance to get stolen by a third party and can be used in unethical works.  In order to mitigate this factor, in the national DNA database, firewalls and IDS have to be implemented to get better security. The actions which can be considered, for instance, relocating the devices to the other network subnet as well as installing the end-to-end encryption to preserve the volatile data of the DNA database. |

# **Chapter 6: Conclusion and recommendations**

This is evident from this paper that, the potential risks can impact the National DNA Database Case Study Project severely, where the data breaches, reluctance to change and integrating issues can be proven as three obstacles towards successfully accomplishing this paper. This study has also advised that mitigation strategies will be the most suitable risk response strategies against the risks. The possible recommendations on behalf of this scenario are mentioned below

* NDNAD or the government needs to employ more skilled IT experts who reduced the challenges of integration of this DNA database by developing a proper integration strategy.
* Also, employing educated and adept workers in this National DNA Database Case Study Project will be proven helpful for dealing with non-compliance and mismanagement issues and can enhance adaptability among the patients by increasing awareness programs.
* Finally, installing a firewall, end-to-end encryption and relocating the devices to different network subnets could be helpful in dealing with data breaches or system failure.

# 

# **Reference list**

Ahmad, Z., Shahid Khan, A., Wai Shiang, C., Abdullah, J. and Ahmad, F., 2021. Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies*, *32*(1), p.e4150.

Chen, H., Pendleton, M., Njilla, L. and Xu, S., 2020. A survey on ethereum systems security: Vulnerabilities, attacks, and defenses. *ACM Computing Surveys (CSUR)*, *53*(3), pp.1-43.

Gerke, S., Minssen, T. and Cohen, G., 2020. Ethical and legal challenges of artificial intelligence-driven healthcare. In *Artificial intelligence in healthcare* (pp. 295-336). Academic Press.

Helo, P. and Shamsuzzoha, A.H.M., 2020. Real-time supply chain—A blockchain architecture for project deliveries. *Robotics and Computer-Integrated Manufacturing*, *63*, p.101909.

Kerman, A., Borchert, O., Rose, S. and Tan, A., 2020. Implementing a zero trust architecture. *National Institute of Standards and Technology*, *2020*, pp.17-17.

Macrae, C.F., Sovago, I., Cottrell, S.J., Galek, P.T., McCabe, P., Pidcock, E., Platings, M., Shields, G.P., Stevens, J.S., Towler, M. and Wood, P.A., 2020. Mercury 4.0: From visualization to analysis, design and prediction. *Journal of applied crystallography*, *53*(1), pp.226-235.

Subriadi, A.P. and Najwa, N.F., 2020. The consistency analysis of failure mode and effect analysis (FMEA) in information technology risk assessment. *Heliyon*, *6*(1), p.e03161.

Taylor, P.J., Dargahi, T., Dehghantanha, A., Parizi, R.M. and Choo, K.K.R., 2020. A systematic literature review of blockchain cyber security. *Digital Communications and Networks*, *6*(2), pp.147-156.

*The Guardian* (2009) *The Guardian*. Guardian News and Media. Available at: https://www.theguardian.com/news/datablog/2009/mar/09/dna-database-ukcrime (Accessed: January 5, 2023).