**Name: Srilekha Napa Ugandhar**

Table of Contents

[Project Description 2](#_Toc506895714)

[1.A SQL login and a password for establishing a connection for Oracle’s SQL developer and MySQL; 3](#_Toc506895715)

[2.The roles and priveleges for the SYSDBA and IT Manager of the KLJ Corporation. 3](#_Toc506895716)

[3.A grant to Joe I.T. King, a cost accountant, to insert, select and update the KLJAsset file 3](#_Toc506895717)

[4.An XOR encryption of the phrase “KLJ will purchase IBM next Monday” 4](#_Toc506895718)

[5. A complete network policy for the KLJ corporation (located in Chicago, Illinois) that specializes in hardware and software development. The organization, which has 1000 employees, contains databases on employees (HR), on the company’s intellectual property assets (patents, trademarks, copyrights, and trade secrets), on their sales, on their inventory, and on their customers and vendors. The company’s communication network involves wired and wireless connectivity, smartphones, VoIP, intercom devices. KLJ executives do not want their employees using the company’s equipment for personal use at any time. 4](#_Toc506895719)

[6. KLJ plans on moving to a suburban industrial park, with five buildings on the campus. Draw the potential property with adequate (and labeled) physical security. 9](#_Toc506895720)

[7. Conduct a risk assessment spreadsheet that contains a list of all possible threats that may affect the KLJ corporation’s databases. The assessment should be presented as a report. 9](#_Toc506895721)

[8. A security plan that will be called into action when a database breach has been detected. 10](#_Toc506895722)

[9.KLJ is considering the use of NoSQL for its inventory. Support the use of NoSQL but keeping database security risk at a minimum. 12](#_Toc506895723)

[10.A conclusion representing the results of your security measures and assessment directed to the client. 15](#_Toc506895724)

[TOE Spreadsheet 15](#_Toc506895725)

[References: 16](#_Toc506895726)

## Project Description

KLJ is a multi-million-dollar software development corporation, specializing in web and business application development, robotics, and health instrumentation design. They are located at 3300 So. Federal St., Chicago, IL 60616.

1. A SQL login and a password for establishing a connection for Oracle’s SQL developer and MySQL;
2. The roles and privileges for the SYSDBA and IT Manager of the KLJ Corporation.
3. A grant to Joe I.T. King, a cost accountant, to insert, select and update the KLJ Asset file
4. An XOR encryption of the phrase “KLJ will purchase IBM next Monday”
5. A complete network policy for the KLJ corporation (located in Chicago, Illinois) that specializes in hardware and software development. The organization, which has 1000 employees, contains databases on employees (HR), on the company’s intellectual property assets (patents, trademarks, copyrights, and trade secrets), on their sales, on their inventory, and on their customers and vendors. The company’s communication network involves wired and wireless connectivity, smartphones, VoIP, intercom devices. KLJ executives do not want their employees using the company’s equipment for personal use at any time.
6. KLJ plans on moving to a suburban industrial park, with five buildings on the campus. Draw the potential property with adequate (and labeled) physical security.
7. Conduct a risk assessment spreadsheet that contains a list of all possible threats that may affect the KLJ corporation’s databases. The assessment should be presented as a report.
8. A security plan that will be called into action when a database breach has been detected.
9. KLJ is considering the use of NoSQL for its inventory. Support the use of NoSQL but keeping database security risk at a minimum.
10. A conclusion representing the results of your security measures and assessment directed to the client.

## 1.A SQL login and a password for establishing a connection for Oracle’s SQL developer and MySQL;

CREATE User Orc\_SQL\_Dev IDENTIFIED BY SQL\_Pwd.

CREATE User MySQL\_Developer IDENTIFIED BY MYSQL\_Pwd

## 2.The roles and priveleges for the SYSDBA and IT Manager of the KLJ Corporation.

Create Role SYSDBA IDENTIFIED BY SysDb

Create Role IT\_Manager identified by IT\_Manager

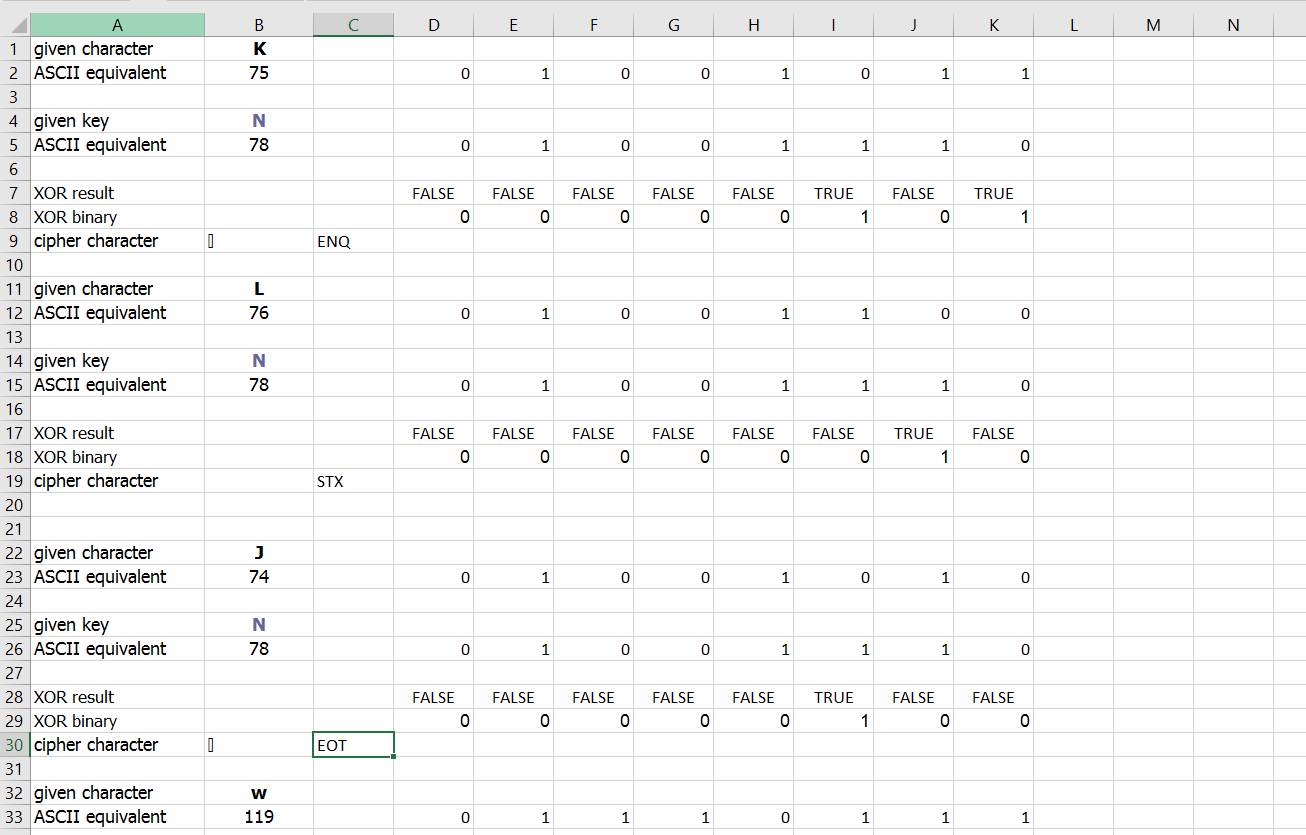
Grant all to SYSDBA

Grant all privileges to IT\_Manager

## 3.A grant to Joe I.T. King, a cost accountant, to insert, select and update the KLJAsset file

GRANT Select, Insert ,Update ON Database TO ITManager

## 4.An XOR encryption of the phrase “KLJ will purchase IBM next Monday”



Please refer attached spread sheet

## 5. A complete network policy for the KLJ corporation (located in Chicago, Illinois) that specializes in hardware and software development. The organization, which has 1000 employees, contains databases on employees (HR), on the company’s intellectual property assets (patents, trademarks, copyrights, and trade secrets), on their sales, on their inventory, and on their customers and vendors. The company’s communication network involves wired and wireless connectivity, smartphones, VoIP, intercom devices. KLJ executives do not want their employees using the company’s equipment for personal use at any time.

**KLJ CORPORATION**

**Network Policy**

**PURPOSE**

The purpose of this policy is to devise procedures and technical guidance to ensure the protection of data and confidential information handled by the computer networks of KLJ corporation.

**SCOPE**

This policy is devised to all who access KLJ corporation’s computer networks. The word “user” in this document will be used to represent all such individuals collectively. This policy is also applicable to all computer and data communication systems owned by or administered by KLJ corporation or its associated organizations.

**POLICY**

All information sent and received over KLJ corporation computer networks that has not been typically found as the property of other parties will be considered as though it is a KLJ corporation’s asset. The policy of KLJ corporation is to prohibit and control unauthorized access, theft, modification, disclosure, destruction, duplication, diversion, loss, or misuse of this information. Also, it is the policy of KLJ corporation to protect information that belongs to third parties that have been entrusted to KLJ corporation in a manner consistent with its sensitivity and in accordance with all applicable agreements of confidentiality.

**RESPONSIBILITIES**

The Chief Security Officer (CSO) is responsible for maintaining and administering the entire organization’s information systems policies, standards, guidelines, and procedures. The responsibility for information systems security is centralized for all of KLJ corporation in the Information Technology department on a daily basis. This department will perform activities necessary to assure a secure information systems environment. The Security Manager is responsible for coordinating investigations into any network safety compromises, incidents, or problems. Besides allocating required resources and employee time to meet the requirements of these policies, departmental managers are responsible for ensuring that all employee users are aware of KLJ corporation policies related to computer and communications system security.

**SYSTEM ACCESS CONTROL**

**End-User Passwords**

KLJ corporation has an obligation to protect the personal and financial information entrusted to it by employees and partners. Using passwords that are hard to guess is key step toward effectively fulfilling that need. Any password used to access information stored by KLJ corporation should be at least 8 characters long, must contain at least one uppercase letter and one number or special character. Passwords will expire annually. When a password expires the users should create a new password that is not same as the last two passwords previously used. Passwords may never be shared or revealed to anyone other than the authorized user. The servers should employ user IDs and passwords unique to each user, and user privilege restriction mechanisms with privileges based on an individual’s rank or position.

**Login and Logout Process**

All users must be positively identified prior to being able to use any KLJ servers or communications systems. Identification for internal KLJ corporation networks involves a user ID and password, both of which are unique to an individual user, or an extended user authentication system. If the user doesn’t enter valid credentials his/her account will be locked temporarily and can be fixed later by the IT services department.

**SYSTEM PRIVILEGES**

**Limiting system access**

Based on the employee position and status in the organisation the system will offer data and information access. This shall be monitored by the IT services department. This mainly serves the purpose of keeping trade secrets intact and make the business up and running for a period of business.

**Granting system access**

The IT services department is authorized to grant access when requested with valid approach. IT services shall bear full responsibility for careful considerations of these requests before granting access to the billable information shared. The privileges granted to users, based on their role within the organization, should be re-evaluated by IT services department annually. In response to feedback from executive’s managers, the HR department, or the IT Services director, system administrators must promptly revoke all privileges no longer needed by users.

**COMPUTER VIRUSES, WORMS, AND TROJAN HORSES**

Users must keep approved anti-virus software enabled on their computers. This software must be used to scan all software coming from third parties. Users are responsible for damage occurring because of viruses on computer systems. As soon as a virus is detected, the involved user must immediately call IT services to assure that no further infection takes place. Software downloaded from untrusted sources must not be used unless it has been subjected to a testing by antivirus software approved by the IT Services director.

**LAPTOPS**

Employees in the possession of portable, laptop, notebook, tablet and other portable computers containing Confidential information must not leave these computers at workplace any time unless the information is stored in encrypted form. Whenever Confidential information is written to a disk or other storage media, the storage media should be suitably marked their names. When not in use, this media should be stored properly in a safe.

**PRINTING**

Printers must not be left unattended if Confidential information is being printed. The persons attending the printer must be authorized to examine the information being printed. Unattended printing is permitted if the area surrounding the printer is protected such that persons who are not authorized to see the material being printed may not enter.

**PRIVACY**

All the mails shared throughout the organisation is encrypted but however these conversations can be accessed with permission from the IT services department for security purposes.

**LOGS**

Appropriate logs for all the employees should be maintained. These logs are to be deleted annually to avoid stacking of data in the servers. However, the snippets of codes to retrieve information shall be added as a comment and the deleted data shall be held at a private data warehousing facility for inventory purposes.

**WEBSITES**

Employees are forbidden to use any kind of social networks or electronic mails during office hours. Websites not appropriate to the working environment will also be blocked for employee access.

**INTERNET**

All employees will have internet access up to a speed of 100Mbps. Internet should be available 24 hrs.

**HARDWARE SECURITY**

The hardware installed in the facility shall be administered by qualified hardware personnel and shall never be modified or changed by the employee.

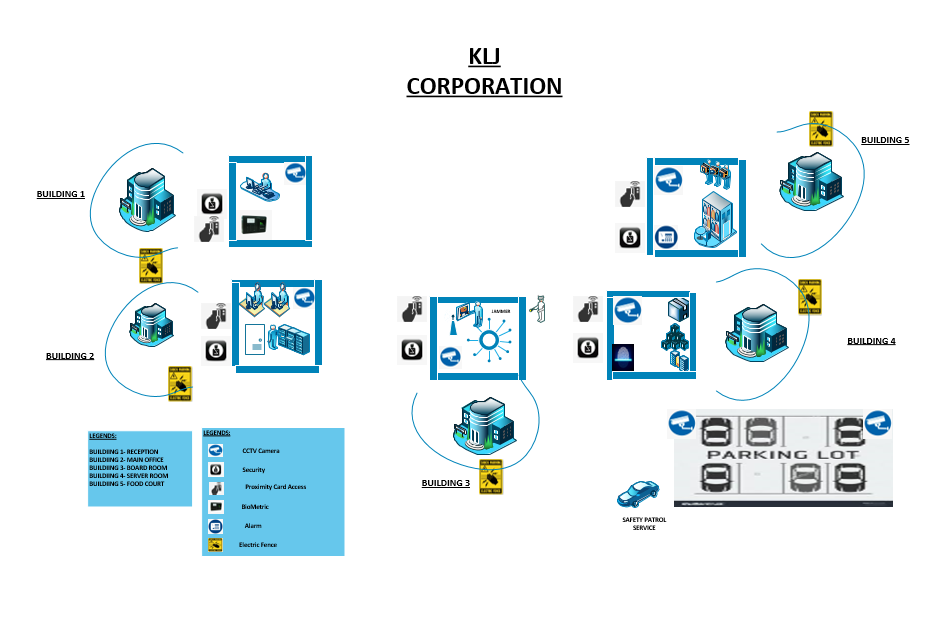
**WIRELESS NETWORKS**

Wireless networks are to be protected from unauthorized user access by passwords which is to be shared among only the individuals using the wireless network.

**CLIENT INFORMATION**

The client information and database security system must be enabled and an automatic security breach sensing system must be installed to ensure maximum safety to the customer records.

## 6. KLJ plans on moving to a suburban industrial park, with five buildings on the campus. Draw the potential property with adequate (and labeled) physical security.



## 7. Conduct a risk assessment spreadsheet that contains a list of all possible threats that may affect the KLJ corporation’s databases. The assessment should be presented as a report.

Please refer Excel Spread sheet

## 8. A security plan that will be called into action when a database breach has been detected.

Security breaches are usually defined when there has been a demonstrated compromise of a security policy and are often associated with incidents of a malicious nature. A data breach takes place when there is an impact related to the data (in the sense of personal data), such as the data being lost or illegitimately accessed, and effects have repercussions not only on the security of the system but also on the right to the protection of personal data of the individual affected

First step is to know what kind of data was breached and the list of potential customers who may get affected due to that breach. It is always a better option to be transparent with the customers rather than to handle the breach as a closed incident within the organization. But before presenting any information to the customers and how they are affected, the problem needs to be first identified properly by the organization.

Incidents can have a variety of root causes, including environmental conditions, such as: storms or floods, human error, malicious attacks, hardware or software failures, and third party failures.Understanding what caused an incident or breach can be technically challenging. Primary investigation needs to be carried out in understanding and obtaining the data that is breached and situations that could possibly result in due to the breach. Impact Assessment, if done proper, provides necessary information to go ahead with the next set of plans and possible solutions that can be implemented. Specific risk management decisions and activities need to be enacted based on the estimated impact.

Potential reasons for the data breach may include :

* Unauthorized users
* Unauthorized access to data
* Eavesdropping on communications
* Corruption of data
* Denial of service
* Complexity to user
* Complexity to administrator
* Lack of accountability
* Overly broad access to data
* Too many accounts
* Operating system break-in

The most important tool to perform risk assessment would be using forensics to identify the problem and the root cause of it. Engineers can use forensics to analyze traffic and instantly determine the root cause of an event, entirely removing guesswork and problem reproduction from the equation. Effective forensics provide these four key capabilities:

* Data Capture: Capture all traffic, 24x7, on even the fastest links
* Network Recording: Store all packets for post-incident, or forensic analysis
* Search and Inspection: Enable administrators to comb through archived traffic for anomalies and signs of problems
* Reporting: Through data capture and analysis, results of investigations are logged and network vulnerabilities are reviewed and analyzed post-mortem.

The next key step after risk assessment would be communication. Both internal and external (if necessary) communication should be encouraged by any organization in case any event of data breach likely occurs.

Basic rules in this case are:

* Be open and sincere. Admit if the fault was on company's side and accept responsibility.
* Provide details. Explain why the situation took place.
* Mitigate. Make conclusions out of the disaster and describe solutions for affected users. If possible, prepare a special offer for the affected audience.
* Educate. Explain how to prevent similar issues in the future.
* Invite to dialogue. Involve your clients, industry experts, analysts, media people and public to the broader discussion about the source of the problem.
* Usually, such approach will allow not only to minimize the negative impact of an IT security accident, but (when implemented correctly) will show your company as the reliable and transparent partner, which is able to operate correctly even during the crisis.

Once the details are communicated, the next step would be to figure how to deal with the data breach. If it is account details, then it is strongly recommended that all the users affected are broadcasted about the issue and asked to change their password immediately. This can block the hackers or any personnel who attached the system to slow down obtaining their account details. An upper level protection would be to lock all the accounts right after the data breach is identified, so that the organization can ensure minimal leak of personal data of the users / individuals, also ensuring unauthorized access by use of the breached information. Everyone can then later be provided with a new temporary password so that they can change it after their login. But before providing any such remedies, it is essential that the root cause is analyzed and the system is fixed to be repellant to such attacks if to happen again. Otherwise, there is no point in enacting such protection measures.

In case of any personal or sensitive data leak, the concerned person whose information has been leaked should be informed right after it is identified, so that other necessary measures (like getting a police report, filing an FTC, etc.) can be taken to minimize the possible attacks that can be performed.

Assigning separate teams to each department would be a good practice as they could concentrate on individual tasks at their hand. Documenting every step from the start of the issue till the resolution would help if some similar issue occurs in the future. Also, it would aid in taking proactive steps by analyzing their level of security as to why the breach happened and how to prevent such breaches in the future. One more thing to remember. The data breach response plan is a living document. As individuals change roles and as the organization evolves (mergers, acquisitions, divestitures etc.) the plan needs to change as well.

To not over-react or make irrational decisions in recovering from the breach. There are a few key steps (in order of importance) that the company should take:

* Investigate the incident. Gathering information on the incident is important in validating that an incident has occurred (i.e., who, what, where, and when the incident occurred)
* If the breach is valid, inform management with a summary of the incident
* Identify the suspected cause of the incident.
* Isolate the effected system and eradicate the cause of the breach
* Implement policy, procedures, and technology if necessary, to prevent a recurrence
* Perform period technology audit or risk assessments combined with network penetration testing to identify weaknesses in the system.

Containing the incident, communicating effectively with vested parties and learning from mistakes are all important next steps once an incident has been identified. Lastly, identifying the impact of compromised assets is critical. After all, effective response to a data breach can mean the difference between minimized impact and closing the doors for good .

## 9.KLJ is considering the use of NoSQL for its inventory. Support the use of NoSQL but keeping database security risk at a minimum.

One major advantage that NoSQL has over other database models is the support for unstructured text. Majority of the data is most enterprise systems are unstructured. The handy part of NoSQL comes in where it can handle indexing of unstructured text either as a native feature or as an integrated set of services. Being able to manage unstructured text greatly increases information and can help organizations make better decisions. NoSQL databases are not a direct replacement for a relational database management system (RDBMS). For many data problems, though, NoSQL is a better match than an RDBMS [4].

Most of the data between systems fly as messages. The typical formats include binary, XML or JSON document. The ability to store these data natively in NoSQL database reduces the code conversion from the source data format, thus lessening the time for ETL (Extract, Transform and Load) .

NoSQL can handle the change over time. It is usually not easy to make big changes to the data model of an RDBMS. Changes must be carefully managed and may even necessitate downtime or reduced service levels. Thanks to the agnostic nature of NoSQL, it can manage change. Also, NoSQL can handle partitioning of database over several servers. So, if the storage requirements go up in the future, it is easy to add inexpensive servers and connect them to the database cluster. When data is not directly related to any other data you can store it anywhere. That means that you can handle more data by adding additional nodes.

NoSQL databases enjoy a quick pace in terms of development and maturation. New features are released all the time, and new and existing features are updated frequently. High end RDBMS systems are generally maintained by highly trained DBAs. But NoSQL databases are designed from the ground up to require only less management using such desirable features as automatic repair, data distribution, and simpler data models leading to lower administration and tuning requirements. However, caution needs to be exercised, since it is a developing model and support may not be available readily. It is easier to find experienced RDBMS programmers or administrators than it is to find a NoSQL expert.

Another advantage of NoSQL is the support for different data models, unlike relational databases which lack explicit data schemes. NoSQL also provides consistency allowing to set the level as well. NoSQL databases have a relaxed, or even non-existent, data model restrictions. It allows the application to virtually store any structure into the database. The result is that application changes and database schema changes do not have to be managed as one complicated change unit. In theory, this will allow applications to iterate faster, though, clearly, there can be undesirable side effects if the application fails to manage data integrity . NoSQL database systems are designed to provide real-time performance while managing large volumes of data.

As enterprises continue to adopt NoSQL more broadly, the question of security will continue to be raised. There is nothing inherent to the NoSQL market that makes it less, or more, secure that relational databases. It is true that some relational database, by aegis of their age and maturation, have more expansive security tooling available . Currently, NoSQL databases are in the evolutionary stage of their lifecycle and, unlike their RDBMS counterparts, such as DB2, MySQL, Oracle and SQL Server, the attack vectors for NoSQL databases aren’t well mapped out. And it’s likely new attack vectors will emerge that will target NoSQL data stores in new ways. More specifically, data breaches caused by a NoSQL injection are probably not far away.

Because most of the popular NoSQL databases are open source, IT staff would be wise to devote some time to contributing stronger authentication and encryption systems to their NoSQL implementations, rather than waiting for the publisher of a proprietary database to make changes. NoSQL data stores are basically vulnerable to the same security risks as traditional RDBMS data stores, so the usual best practices for storing sensitive data should be applied when developing a NoSQL-based application. These include:

* Encrypting sensitive database fields;
* Keeping unencrypted values in a sandboxed environment;
* Using sufficient input validation;
* Applying strong user authentication policies.

Of course, it would be ideal if there were an accepted standard for authentication, authorization and encryption in the yet-to-mature NoSQL space. Until such a standardized consensus can be reached, the best approach is to look at security in the middleware layer, rather than on the cluster level, as most middleware software comes with ready-made support for authentication, authorization and access control.

There are multiple facets to using encryption to protect data at rest inside a NoSQL system. Hadoop prefers to do this by adding encryption at the HDFS level. Thus, encryption is transparent to applications, but fine-grained controls can be added later on . Using existing authentication systems like Active Directory to enforce access to a NoSQL system from the outside is also a good measure to enhance security. But, Authentication and Encryption is almost nonexistence or is very weak when implemented.

The following are security issues associated with NoSQL databases:

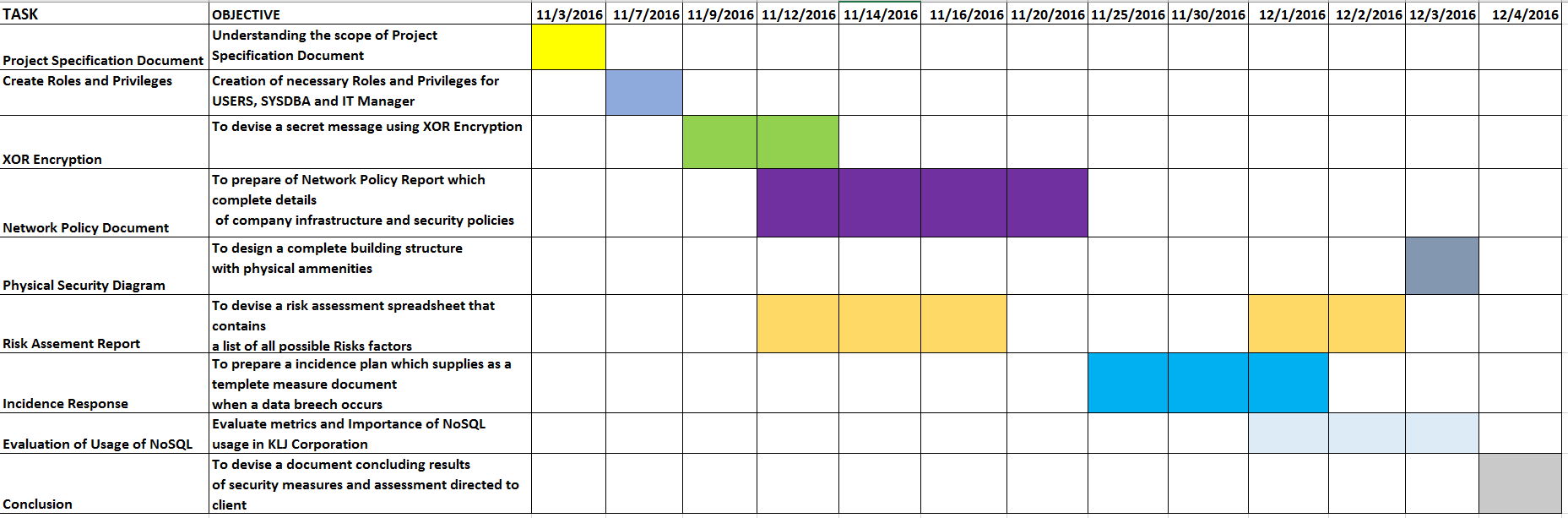
* Administrative user or authentication is not enabled by default.
* Very weak password storage
* Client communicates with server via plaintext
* Cannot use external encryption tools
* Lack of encryption support for the data files
* Weak authentication both between client and the servers
* Vulnerability to SQL injection
* Denial of service attacks.
* Unencrypted data at rest.
* The Available encryption solution isn’t production ready
* Encryption isn’t available for client communication.

With all this security problems, it best to understand that NoSQL databases are still new technologies and more security enhancements will be added to newer version. Every new technology is susceptible to all kind of security risks initially, until a base for security is framed. NoSQL is a developing technology with lot of scope and enhancements to be performed on it. Given the advantages of NoSQL over conventional database systems, the security risks are not so high comparatively, since same risks prevail in both the technologies. With proper strategy and necessary security measures in place, NoSQL can be a very productive and a cutting-edge tool that could serve the organization with various benefits it holds uncovered and within.

## 10.A conclusion representing the results of your security measures and assessment directed to the client.

Design and Implementation of Safeguards and analysis described above shall apply to all methods of handling financial information, whether in electronic, paper or other form. The IT Services department and CSO will implement safeguards to control the risks identified through such assessments on a regular basis and too often test or otherwise monitor the effectiveness of such security measures. Such monitoring may be accomplished through existing network testing and problem escalation procedures. The IT Services CSO shall coordinate with those responsible for the third-party service procurement activities among the Information Technology services desk and other affected departments to raise awareness of, and to devise methods for, highlighting only those service providers that can maintain appropriate safeguards for financial information of employees and other third parties to which they will have access. These standards shall apply to all existing and future contracts entered with such third-party service providers. Adjustments to Program the IT Services CSO is responsible for evaluating and adjusting the Program based on the risk identification and assessment activities undertaken in pursuit of the Program, as well as any material changes to the Institution's operations or other circumstances that may have a circumstantial impact on the Program. These policies will thus ensure maximum network security and safety of the database of KLG corporation as well as the patents own by the organization. It also ensures safekeeping of employee data and confidential business secrets intact within the organization. It also ensures limited access to a certain high-ranking official to only access such information thereby providing state of the art security to the organization.

## TOE Spreadsheet



Please Refer Excel Spreadsheet.

## References:

Retrieved from Website: <http://www.europarl.europa.eu/studies>.

Retrieved from Website: <http://docs.oracle.com>.

Retrieved from Website: <http://digitalguardian.com/blog>.

Retrieved from Website: <http://www.dummies.com/programming/big-data>.

Retrieved from Website: <http://tekedia.com>.

Retrieved from Website: <http://www.techrepublic.com/blog>.

Retrieved from Website: <http://basho.com>.

Retrieved from Website: <http://www.computerweekly.com>.