Research, Analysis, Implementation, of Security measures and Risk Assessment for KLJ Corporation

Course Name : ITMS 528 Database Security
Semester : Fall 2016
Professor Name : Prof. Katherine Papademas
Student Name : Manthan Sudhir Kapadia
Date of Submission : December 3, 2016

OBJECTIVE:

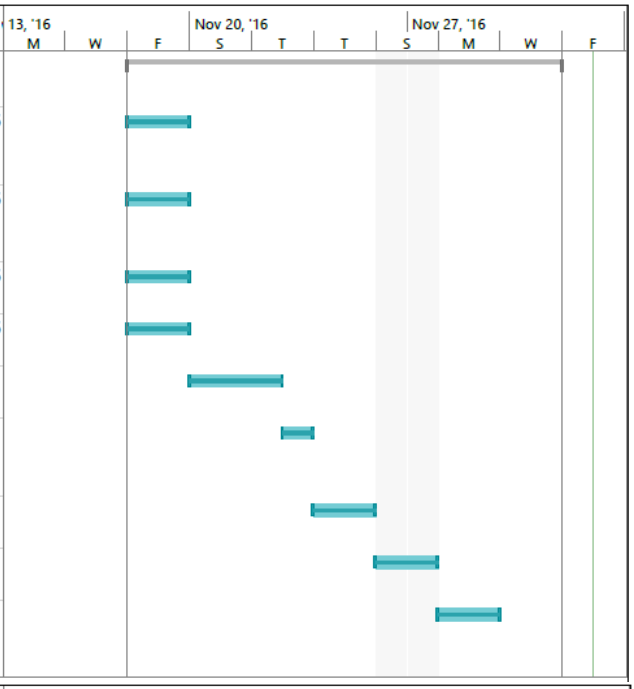
To research, study and do analysis for KLJ Corporation. The area of research, study and analysis includes database management, implementation of security measures, framing of network security policy, designing of physical security architecture, last but not the least, risk management.

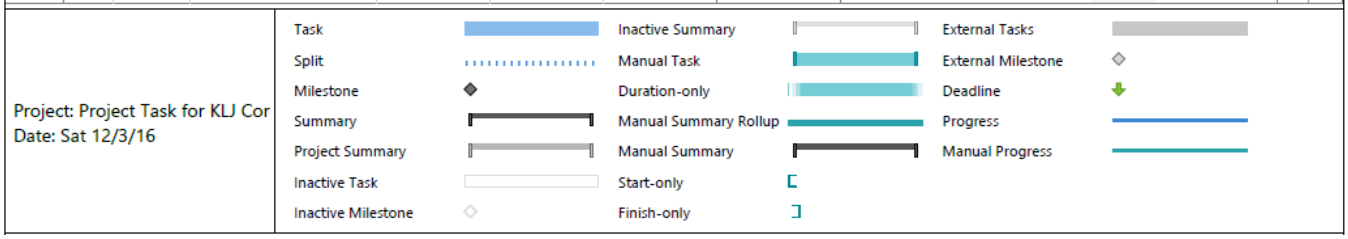
Client Name: KLJ Corporation,
3300 So. Federal,
Chicago, IL 60616.

Title of Contents:

Project task report for KLJ Corporation:

ID	Task Mode	Task Name	Duration	Start	Finish
0		**Project Task for KLJ Corporation**	**10 days**	**Fri 11/18/16**	**Thu 12/1/16**
1		Creation of SQL login and password for establishing	2 days	Fri 11/18/16	Sat 11/19/16
2		Assigning roles and privileges for SYSDBA and IT	2 days	Fri 11/18/16	Sat 11/19/16
3		Assigning grants to access KLJ asset	2 days	Fri 11/18/16	Sat 11/19/16
4		XOR encryption of the phrase	2 days	Fri 11/18/16	Sat 11/19/16
5		Network Policy for KLJ Corporation	3 days	Sun 11/20/16	Tue 11/22/16
6		Physical security diagram for KLJ Corporation	1 day	Wed 11/23/16	Wed 11/23/16
7		Risk assessment for KLJ Corporation	2 days	Thu 11/24/16	Fri 11/25/16
8		Security plan in event of Data	2 days	Sat 11/26/16	Sun 11/27/16
9		Consideration of NoSQL for KLJ Corporation's	2 days	Mon 11/28/16	Tue 11/29/16
10		Conclusion representing results of security measures	2 days	Wed 11/30/16	Thu 12/1/16





Creation of SQL login and password for establishing connection to KLJ Corporation's database:

```
create login KLJ_Corp
with password = 'pwd123' must_change,
check_expiration = on;
```

Assigning grants, roles and privileges:

- Creating user named SYSDBA
  create user SYSDBA identified by #klJsysdb@;

- Granting roles and privileges to user SYSDBA :
  grant connect, resource, dba to SYSDBA;

- Assigning all privileges to SYSDBA:
  grant all privileges to SYSDBA;

- Creating user named ITMgr:
  create user ITMgr identified by #itMgr@J;

- Granting roles and privileges to IT Manager in KLJ Corporations database named db_klj:
  grant insert, select, update on db_klj.* to ITMgr;

- Creating user Joe, cost accountant of KLJ Corporation and granting him privileges:
  create user Joe identified by #itKngcst@cc
  grant insert, select, update on KLJAsset to Joe;

XOR encryption of important information of KLJ Corporation:

Kindly refer to the XOR Encryption attached in drop-box.

XOR Encryption.xlsx

Network Security Policy for KLJ Corporation:

This network security policy of KLJ Corporation is applicable on global level and the aim of this network policy is to secure KLJ Corporation's business requirements by supporting its infrastructure and implementing methods which contribute in reducing risk. Global infrastructure department, Global systems security, Site infrastructure department, Site systems security, group of managers, several user groups from HR department are all responsible for maintaining the policy so that it is updated and relevant.

Root security policy of KLJ corporation provides enough protection, confidentiality, and integrity of all the corporate data, software, storage media, systems, be it local or remotely ensuring hundred percent availability and reliability to all authorized staff member.

Root security policy of KLJ corporation comprises of subordinate policies:

- **Acceptable use of technology:**
  This policy covers fair usage of technology ie. desktop, server, systems, mobile, laptops by employees and contractors as well. It includes following list of things which needs to followed:
  - Only that person can access system to whom ownership is granted
  - KLJ Corporation systems should be strictly be used for business use and not non-business use
  - The user should have authorization to use system,
  - All the employees must use KLJ Corporation's encryption method to protect data,
  - No system personalization is allowed. Only KLJ Corporation's customized image is allowed
  - All employees must follow KLJ Corporation's password policy
  - Only licensed software must be used. No usage of freeware permitted

- **Email Policy:**
  This policy covers usage of KLJ Corporation's email address and mailbox. It includes following list of things which needs to followed:
  - Fair usage of KLJ Corporation's email id
  - Usage of of KLJ corporation's email id other than business use is restricted
  - There should be no illegal transmissions, chain letters
  - No other email id apart from KLJ Corporation's should be used
  - All the email traffic is continuously monitored and may lead to consequences if unusual traffic is detected.

- **Web and Internet Policy:**
  This includes what type of browsers needs to be used, their configuration, restrictions on websites, internet-facing gateway configuration, what traffic is allowed in and out and its justification. It includes following list of things which needs to followed:
  - KLJ Corporation implements very strict web filtering imposing restriction on accessing external websites.
  - No access to non-business email accounts via KLJ Corporation's network
  - Uploading of data, media downloads, media streaming is restricted

- Only browsers included in KLJ Corporation's image must be used
- None of the browser configuration should be tweaked
- KLJ Corporation's internet authentication, incoming and outgoing protocols permitted list and rejected list, application-level filtering for HTTP, SMPT traffic and Domain Name Services.

- **Computing and Storage devices:**
  This includes type of computing and storage devices that are allowed or restricted in KLJ Corporation's environment. It includes following list of things which needs to followed:
  - Employees must not bring their PDA to KLJ Corporation
  - Only devices issued by KLJ Corporation for business purpose are allowed access
  - Devices issued by KLJ Corporation must be regularly updated for any patches
  - No personal data must be there on KLJ Corporation's device
  - All the devices issued by KLJ Corporation must be encrypted and password protected
  - Only applications in KLJ Corporation's image are allowed in devices issued by KLJ Corporation

- **Remote Access:**
  This policy includes what kind of information can be accessed in what form and from which place. It includes following list of things which needs to followed:
  - Remote access only to authorized employees
  - Remote access is granted only with specific combination of hardware and software
  - Users who are not authorized to remotely access needs to open a workflow/ service request with Infrastructure Services of KLJ Corporation to grant access
  - Remote access is safeguarded by passwords, security tokens, VPNs
  - Account activity is continuously monitored for suspicious activity

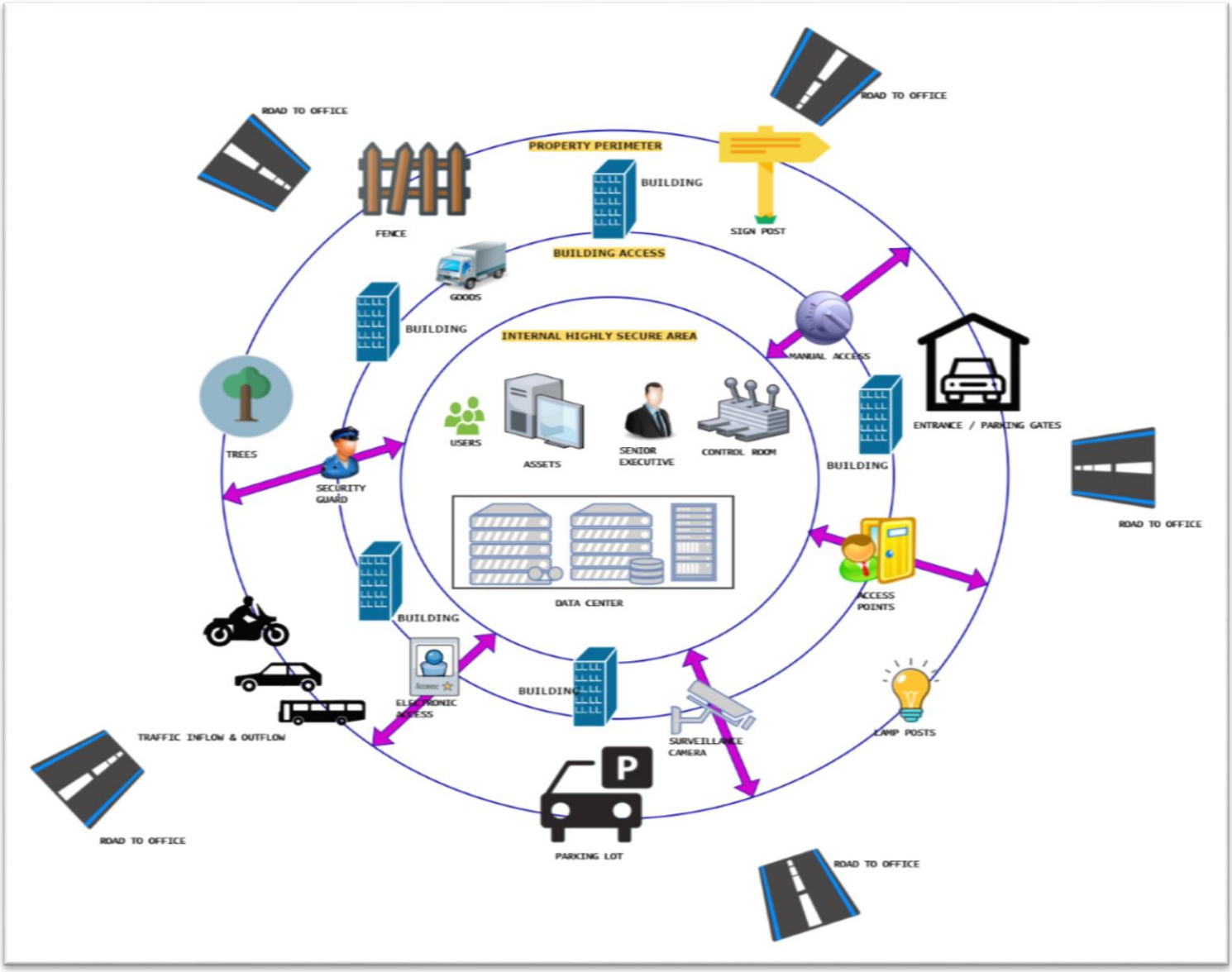
- **Servers:**
  This policy governs servers, services which needs to enabled or disabled and differentiation between test, stage, development, and production servers. It includes following list of things which needs to followed:
  - All the servers of KLJ Corporation have their own role and information categorization which must be stored on server is done based on infrastructure
  - Any deployments or changes on server can be done only by Infrastructure Services employees
  - All the characteristics of server like administrative access, protection, monitoring, OS configuration policies, back-up policies, patch control for server, change control procedures, must be done by authorized Infrastructure Services employee

- **Incident Response Plan:**
  One of the most important part of policy is direction in case of un-avoidable incident, security incident, immediate steps need to be taken, personal who takes care of situation. This policy considers aspects of point of contact during incident, emergency evacuation procedures. It also includes list of people who needs to be connected at the time of incident and they are as follows:

- System and network administrators
- Senior management
- Managed service providers
- Help desk
- Lawyers
- Public relations

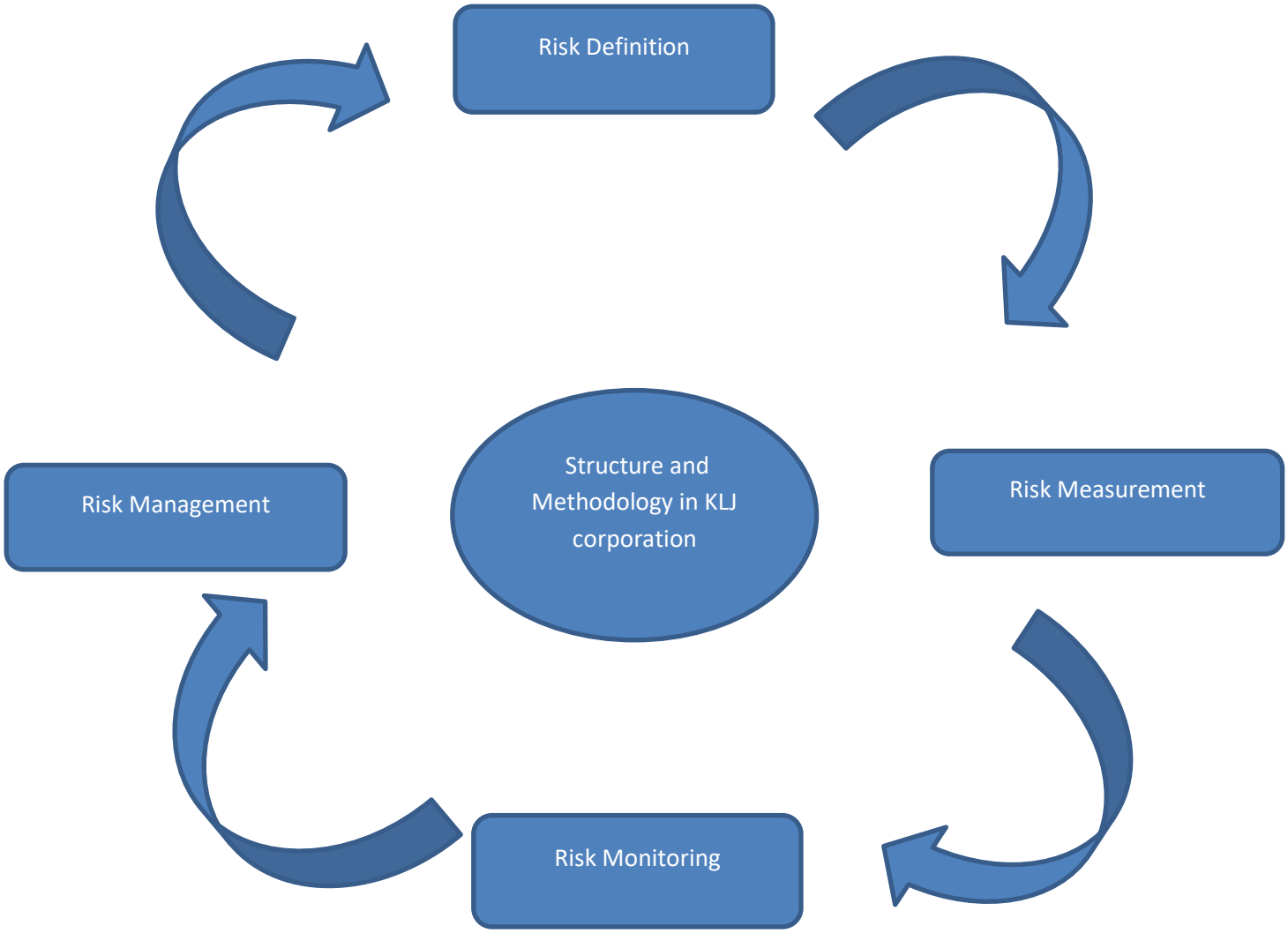
Reference:
Avolio, F. (2007, July). Producing your network security policy. Retrieved November 20, 2016, from http://www.watchguard.com/docs/whitepaper/securitypolicy_wp.pdf

Physical security architecture for KLJ Corporation:

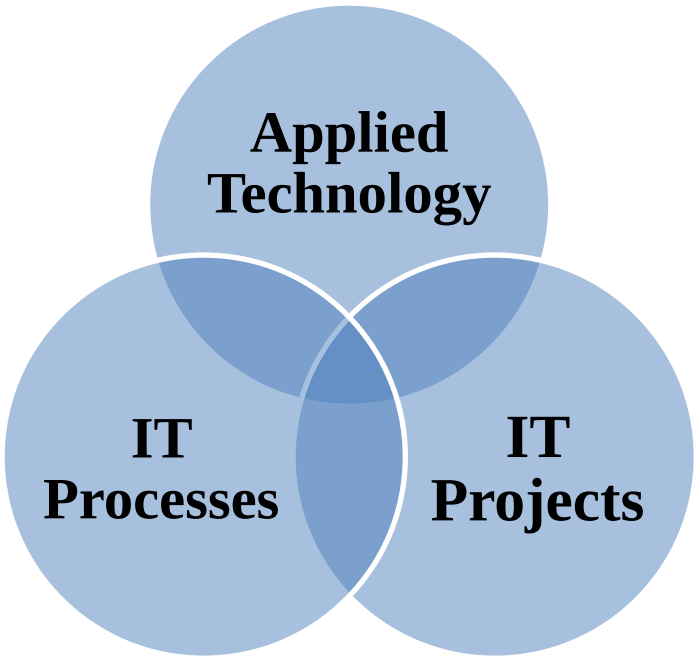


Risk Assessment for KLJ Corporation:

- Risk can mainly be called an un-invited or unplanned activity which gets in due to any loop holes because of inadequate resources, weak processes, humans, system, or any external un-controllable event.
- To prevent any organization from all this, a proper and strong Risk Management framework needs to be implemented.
- This framework is mainly focused in-
  - Risk analysis
  - Enhancing risk response decisions
  - Reducing operational efficiency and losses
  - Calculates control measures
  - Track of safety limits and acceptable risk levels
- KLJ Corporation follows a risk management framework which mainly encompasses four fundamental areas as shown below:



- While creating risk assessment spreadsheet for KLJ corporation, different areas are taken into consideration before creating the report. The figure below covers a bird view on the areas.

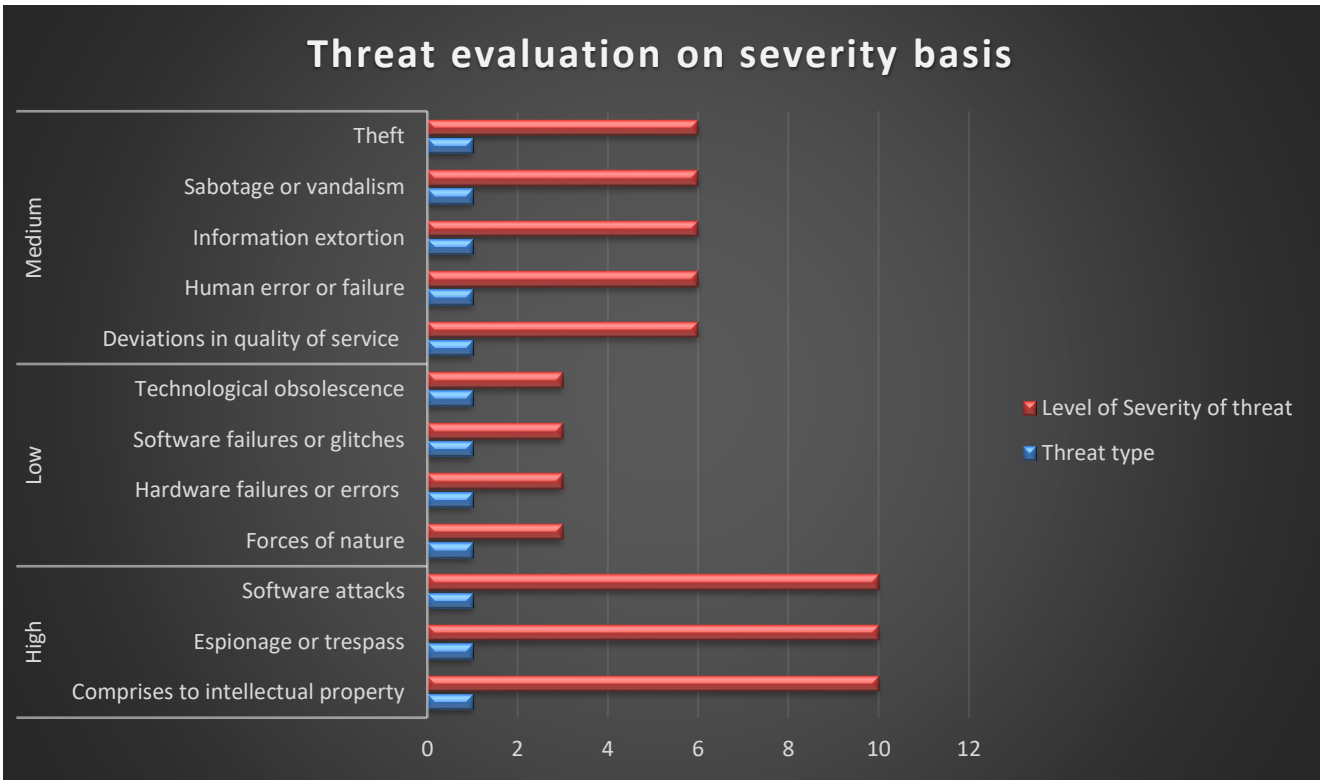


- All these areas have factors which contributes to risk assessment and what should be assessed. The figure below gives an overview on it.

Area	Risk Areas	What to access	
Applied Technolog	Applications, Databases, Operating Systems, Infrastructure Componenets.	Stability, Sensitivity, Financial Exposure, Integrity, Business risk evaluation criteria, Integrity.	From the topmost level, the areas of risk which needs to be accessed, the threats, their rank, mitigation plan everything falls into one or the other area mentioned below- (1) Strategic; (2) Operational; (3) Legal/ Regulatory Compliance; (4) Financial Reporting
IT Processes	Frameworks like ITIL, COBIT, ISO etc. Also process delivery services.	Reliability, Human resoucres, Complexity, Consistency, Efficiency, Technology leverage, Business risk evaluation criteria.	
IT Projects	Any on-going, future, or planned projects that involve strategic initiatives, new technologies, applications, changes to current IT processes	Project budget, criticality, custom programming, project management experience, development platform, process and control engineering, business risk evaluation criteria, executive ownership	

- The list of threats and a bar graph which KLJ corporation's database is prone to is listed below with its level of severity and threat rank.

Level of Severity	Threat	Threat Rank
10	Comprises to intellectual property	High
6	Deviations in quality of service	Medium
10	Espionage or trespass	High
3	Forces of nature	Low
6	Human error or failure	Medium
6	Information extortion	Medium
6	Sabotage or vandalism	Medium
10	Software attacks	High
3	Hardware failures or errors	Low
3	Software failures or glitches	Low
3	Technological obsolescence	Low
6	Theft	Medium



- In the stage of risk analysis, all the threats which the corporation is always prone to should have a valid justification on its level of severity and a mitigation.

RISK ANALYSIS	
Threat	**Justification of Threat Rank**
Comprises to intellectual property	This threat is ranked high as it has a huge impact on economy on international level.
Deviations in quality of service	This threat is ranked medium as any problem related to ISP, Power or WAN service can be mitigated within minimal downtime using backup plans.
Espionage or trespass	This threat is ranked high as any problem related to ISP, Power or WAN trespass can be mitigated within morimal downtime using backup plans.
Forces of nature	This threat is given low priority as the frequency of occurrence of any natural calamity is less.
Human error or failure	This theat is ranked as medium as problems related to human intervention are minimal and can be reduced with proper training and exposure to different work environment.
Information extortion	This threat is ranked medium as it rarely happens only if someone breaks into all layers of security and threatens about information disclosure.
Sabotage or vandalism	This threat is ranked medium as it happens only if someone breaks into all layers of security and threatens about destruction of system and information.
Software attacks	This threat is ranked high as the attack by virus, wormsmalware, denial of service has been increased drastically.
Hardware failures or glitches	This threat is ranked low as hardware is nothing but an electronic device which has an adequate amount of life.
Software failures or glitches	This threat is ranked low as chances of its occurrence is less as during the design and planning stage all the loopholes and code problems are take care of.
Technological obsolescence	This threat is rankek low as infrastructure team of ogranization takes care about updating everything on timley basis.
Theft	This threat is ranked medium as there are chances of thefts inspite of security.

RISK ANALYSIS	
Threat	**Control, Mitigation or Elimination of the Threat**
Comprises to intellectual property	Strong file protection policies which prevents piracy, copyright protection and implementation of security policies.
Deviations in quality of service	Backup line should be kept available which has capability of switching up immediately as soon as one line goes down.
Espionage or trespass	Use of latest authentication standards for identifying the authenticity before granting access.
Forces of nature	Business continuity plan is a must in this case along with regular backup facility depending upon the type of the project.
Human error or failure	Acceptance and followup on all the policies and standard operating procedures.
Information extortion	Taking all sorts of preventive measures to keep dumpster divers away and providing each file a level of encryption depending upon type of files.
Sabotage or vandalism	Effective security practices to prevent unauthorized access and determining who should be given full access over system or information.
Software attacks	Use of updated anti-virus softwares, and following best practices to avoid being infected by virus, worms etc.
Hardware failures or glitches	Timely maintenance activity.
Software failures or glitches	Code review helps to avoid any bugs or loopholes.
Technological obsolescence	Regularly updating all the softwares, machines, application and patches.
Theft	Implementation of technology which provides strong vigilence .

Security plan of action in event of data breach incident:

Security plan that will be called into action when a certain database has been breached and detected is mentioned below:

- **Validating the data breach:**
  Perform a thorough check through the logs and available resources to confirm about occurrence of data breach.
- **Assignment of Incident manager for investigation on validation of data breach:**
  The team manager appoints an incident manager who looks into overall incident response, breach response documentation, reporting process, and managing and controlling flow of information.
- **Assemble incident response team:**
  To start immediate action on breach, a team is created which comprises of masses from management, IT, legal, risk management, finance audit and public affairs. They begin with determining the status of breach as to whether it is on-going, active or post breach so that necessary actions can be taken like secured access, blocking unauthorized access of IT data/ systems etc. All the procedures followed are duly documented down for future references and analysis.
- **Determining the scope and composition of the breach:**
  In case of criminal acts, relevant law enforcement or any Federal, State or Local legal requirements needs to followed regarding enforcement. Identifying all affected data, machines, devices, locations and preserving all electronic logs and records for later forensic examination.
- **Notify the data owners:**
  To foster a co-operative relation between incident response team and data owners, inform them as about data breach as soon as possible. Devise a plan to mitigate the damage, perform analysis and design mitigation strategies to prevent future occurrences and securing sensitive data.
- **Restoring all the business:**
  After all the analysis, next step is to restore the organization by developing and executing a comprehensive and well effective restoration plan. Determining the timeframe and requirements to be taken into consideration for resuming all the operations. The Incident response manager must plan the restoration of all the compromised systems and networks with minimum risk of incident recurrence and impact to existing operations. There should a thorough network monitoring activity on-going to prevent incident recurrence.
- **Retaining the customer and client relationships:**
  Retaining customer and client relationships is very important after a breach incident. Performing post incident analysis, amending the existing process to minimize probability of breach in future, revising, policies, SOPs, procedures, security plans and adequate trainings to staff to prevent incident recurrence.

Reference:

Privacy Technical Assistance Center (PTAC) | U.S. Department of Education. (n.d.). Retrieved November 26, 2016, from http://ptac.ed.gov/Checklist_data_breach_response_092012.pdf

Consideration for usage of NoSQL for inventory of KLJ Corporation:

- KLJ is a multi-million-dollar software development corporation, that specializes in web and business application development, robotics, and health instrumentation design.
- An industry that deals in such type of business needs an environment which has factors mentioned below-
    a. Large number of customers moving online which needs dedicated scaling which helps in meeting needs of millions of customers. Performance requirement is also high with 100% availability and connectivity.
    b. Everything is connected via Internet which involves different data structures, continuous streams of real-time online data, software, and hardware updates.
    c. The data storage is increasing and type of data is varying, in short Big Data is expanding consisting of semi-structured/ unstructured data, data from numerous sources, and data generated by millions of customers.
    d. Cloud connectivity provides un-limited scaling to match requirements of 'n' number of customers, global-level operation, speed, and minimization of infrastructure cost.
    e. As the world, has started accepting mobile transformation, creating offline apps which requires no network connection, compatibility of multiple mobile platforms with single backend and synchronization of mobile data with databases in cloud has boosted.
    f. Facilitating features like automatic repair, simplistic data handling, modelling and tuning which helps in lower maintenance and administration.
    g. Commodity computing expedites management of data explosion and transaction volumes which leads to lower infrastructure cost.
- All the above factors prove strong point for which KLJ corporation should consider moving to NoSQL database.
- To keep database security at minimum, the IT staff must work on security aspect as, NoSQL databases are usually attacked by cyber criminals.
- The best way to build security for NoSQL is by achieving below tasks-
    a. Transparent encryption
    b. Integrated key management
    c. High-performance encryption and data security architecture
    d. Usage of sandbox environment to store unencrypted format
    e. Usage of high level authentication policies

Reference:

Why NoSQL? (n.d.). Retrieved on November 28, 2016, from http://www.couchbase.com/nosql-resources/why-nosql

Conclusion:

As a fact of conclusion of security measures and assessment for KLJ Corporation, effective services were offered to KLJ Corporation. All the tasks were effectively analyzed, researched, and successfully implemented. To conclude, the list below covers all the security measures and assessment directed for all the tasks.

- A safe and secured login to KLJ Corporation's database is created, authorizing access to different aspects of database depending on roles, privileges and grants assigned to different workgroup of employees.
- An important information about KLJ Corporation ie. "KLJ will purchase IBM next Monday" is securely encrypted using XOR encryption.
- Network security policy for KLJ corporation is drafted after thorough check and scrutinizing every aspect of the organization to curb down misuse of data, prevent loss, prevent breaches of CIA, manipulation of data, security threats.
- On the basis on geography of KLJ Corporation, different layers of security and components which should be added in each layer is suggested. All these things are successfully mapped into Physical Security Diagram.
- All the probable risk factors which the KLJ corporation is prone to are studied, mapped down as per their threat rank, justification of threat rank. To effectively work against those risks, risk assessment spreadsheet provides all the mitigation action for KLJ Corporation which helps them to keep threats away.
- Any organization is prone to breaches and attacks and so is KLJ Corporation. Taking into consideration about all sorts of breaches and attacks, a structured security plan is framed for KLJ Corporation which provides quick and lucid plan action in event of such incident.
- As per the additional requirement of KLJ Corporation regarding moving its inventory to NoSQL, a thorough systematic screening of all the workflows regarding inventory management is done for KLJ Corporation. A briefing about advantages of migration to NoSQL is provided to KLJ Corporation along with security risks and mitigation which the Corporation needs to follow to maintain security risk at a minimum.