# Database Risk Management Implementation Plan

- **Create a list of Cybersecurity Implementation controls discussed in class**

- Authentication – User Accounts
    - DBMS – Database Management System is a system for managing databases and its data.
    - Application User – They are general users of the database who only have access to perform Data Manipulation Language (DML) actions.
    - DBA – The configuration and operations of the database are managed Database Administrator
    - Application Owner – Application owner owns all the objects used by an application and assigns users privileges to application objects and application roles.
    - Application User Manager – An Application User Manager oversees and assigns application roles to users
    - Application Account – A specialized account with elevated privileges not intended for general use and used to perform privileged functions.
    - Database Auditor – Database auditor is responsible to manage database audit records and monitor DBA actions.
    - Database Operator – A specialized account with admin privileges for performing functions like backup and database startup.
    - Passwords – Passwords are the most common means of authentication to databases.
    - Certificates – It can be used for authentication only if its configured to meet certificate validation and protection requirements.
    - External Authentication – Databases also support authentication via external authentication servers and can be authenticated in various ways by the DBMS to gain its trust.
    - Credential Storage – Along with all kinds of data, even credentials are stored with the database and require strong encryption policies for its protection. To avoid any potential redirection attacks, database names should be fully defined in the remote connection file.

- Authorization
    - RBAC – Role Based Access Controls are ideal means of authorization as they provide both separation of users and implementation of least privilege.
    - Multi-tier applications – A single database can be used to access the database application for enabling database roles as well as for different user functions.
    - Rename default accounts – Renaming the default account names can limit different kinds of attacks.

- Confidentiality
    - Data Encryption – Data must be encrypted both at rest and in transit to ensure its confidentiality.
    - Application Code – Even application code can be found in databases and should be encrypted to avoid providing sensitive information to a malicious user.
    - Encrypt Data Files – Sensitive data files along with metadata and other config files can be found at local host which demand protection by encryption.
    - Database Configuration, Transaction logs and Audit trails – These are sensitive information which can be abused by malicious actors if not encrypted.

- Data Integrity
    - Transaction Logs – Data Integrity policies require that all transaction logs need to be protected by good encryption techniques.
    - Database Integrity – Database compromises can lead to heavy fines under different regulations and thus need to be safeguarded by encryption controls and failover policies.

- Auditing
    - Audit logs Protections – Audit logs contain sensitive data and needs to be stored outside the database for protection.
    - Audit logs Retention – Audit logs should be retained for a period of time to gain valuable insight and for analysis purposes.
    - Audit Reporting – Any suspicious activity should be notified to the administrators.

- Replication and Federation
    - Database Links – They play a vital role in replication and federation and are used by backup/recovery services.
    - Database Replication – Crucial data can be replicated automatically to a remote database by the use of database links.
    - Federated Databases – Distribution of data across two or more databases is accomplished through use of federated databases.

- Clustering
    - Database Clustering – Clustering provides uninterrupted services to clients by maintaining hot-backup level of availability among two or more databases.
    - Accountability – Actions on a database and its related actions on a remote database can be tracked.
    - Protect Communication Path – For sensitive data, the communication path needs to be protected.

- Backup and Recovery
    - DBMS Backup – To ensure data integrity, Databases need to be backed up regularly.
    - Database Recovery – Databases need to be recovered maintaining integrity in the event of a catastrophe.

- Operating System Protection
    - Database Directories and Files – Disk partitions should be used for storage of directories and files and not to be shared with other applications.
    - Dedicated OS Account – Dedicated OS Accounts should be used for installing and ownership of database software files.
    - Database Software – Database software should be reviewed for unauthorized changes and should be included in system records.

- Application Protection
    - Input Validation – Input validation should be done to avoid compromise of database processes.
    - Review Authentication Method – All the authentication methods used to connect to databases needs to be reviewed.
    - Minimum Privileges – All the accounts used by applications to access the database need to be assigned least privileges.

- Network Protection
    - Network Access Protection – Network Access Protection provides an additional level of protection for database security.
    - Time and Count limits on Network Session Parameters – Limiting such parameters can provide protection against attacks like DOS and session hijacking.
    - Protection against Unauthorized Disclosure – Authentication Credentials can be sniffed on the network if proper security controls are not implemented.

- Security Design and Configuration
    - Procedural Review – A review of all the current database policies and procedures is conducted regularly for effective risk management.
    - Configuration and Specification – A review of all the configurations and specifications is done to safeguard against any known threats and vulnerabilities.
    - Compliance Testing – Any security updates or patches are first tested on test servers before being implemented on actual systems.
    - Functional Architecture for IS Applications – Design of the architectures should be considered before applying the risk management policies.
    - Non-Repudiation – Non-Repudiation is ensured by applying strong cryptographic mechanisms.
    - Partitioning and application – For database security, DBMS should be installed on dedicated hosts.

  - Ports, Protocols and Services – Known and consistent ports, protocols and services which comply with network protection rules should only be used.
  - Configuration Management (CM) Process – Review of all software libraries and database application libraries need to be reviewed.
  - IA Documentation – IA Documentation is nothing but the IA Risk Management Plan.
  - System Library Management Controls – The integrity and availability of all files and directories could be affected if correct policies are not implemented.
  - Security Support Structure Portioning – There can be vulnerabilities when security support structure partitioning is used.
  - Software Baseline – A software baseline for current DBMS should be maintained for monitoring and verification purposes.
  - Group Identification and Authentication – The probability of threat to assets in a database increases when group accounts are involved.
  - Individual Identification and Authentication – Storage is required for an Individual's passwords and attributes.
  - Key Management – secure key management and secure authentication protocols are required.
  - Token and Certificate Standards – Identification & authentication via passwords is not secure, as a result tokens like Common Access Card and PKI certificates are used as a secure means.

- Enclave and Computing Environment
  - Access for Need-to-know – Authorized Access risk management policies are required for securing databases and their computing environment.
  - Audit Record Content – Auditing of all security events are required to detect any unauthorized activities in databases and their computing environment.
  - Audit trail, Monitoring, Analysis and Reporting – Audit trail monitoring, Analysis and Reporting and lead to early detection which is crucial in preventing any kind of attacks.
  - Changes to Data – The ability to restore a database to an original state is crucial when applying security patches or data changes.
  - Encryption for Confidentiality: Data at Rest – Databases may be compromised by attackers; hence encryption is required to safeguard data present in databases.
  - Encryption for Confidentiality: Data in Transit – Data traversing on Weak network can be sniffed by malicious users, hence data in transit should be encrypted.
  - Data Change Controls – Database recovery or rollback helps to preserve the integrity of data in case of incomplete or interrupted transactions.
  - Interconnection among DoD systems and Enclaves – Any system interconnections need to comply with the DoD interface control rules.
  - Audit of Security Label Changes – Security label is assigned to data indicating where this feature is in use. Any changes to this label are an indication of malicious activities.

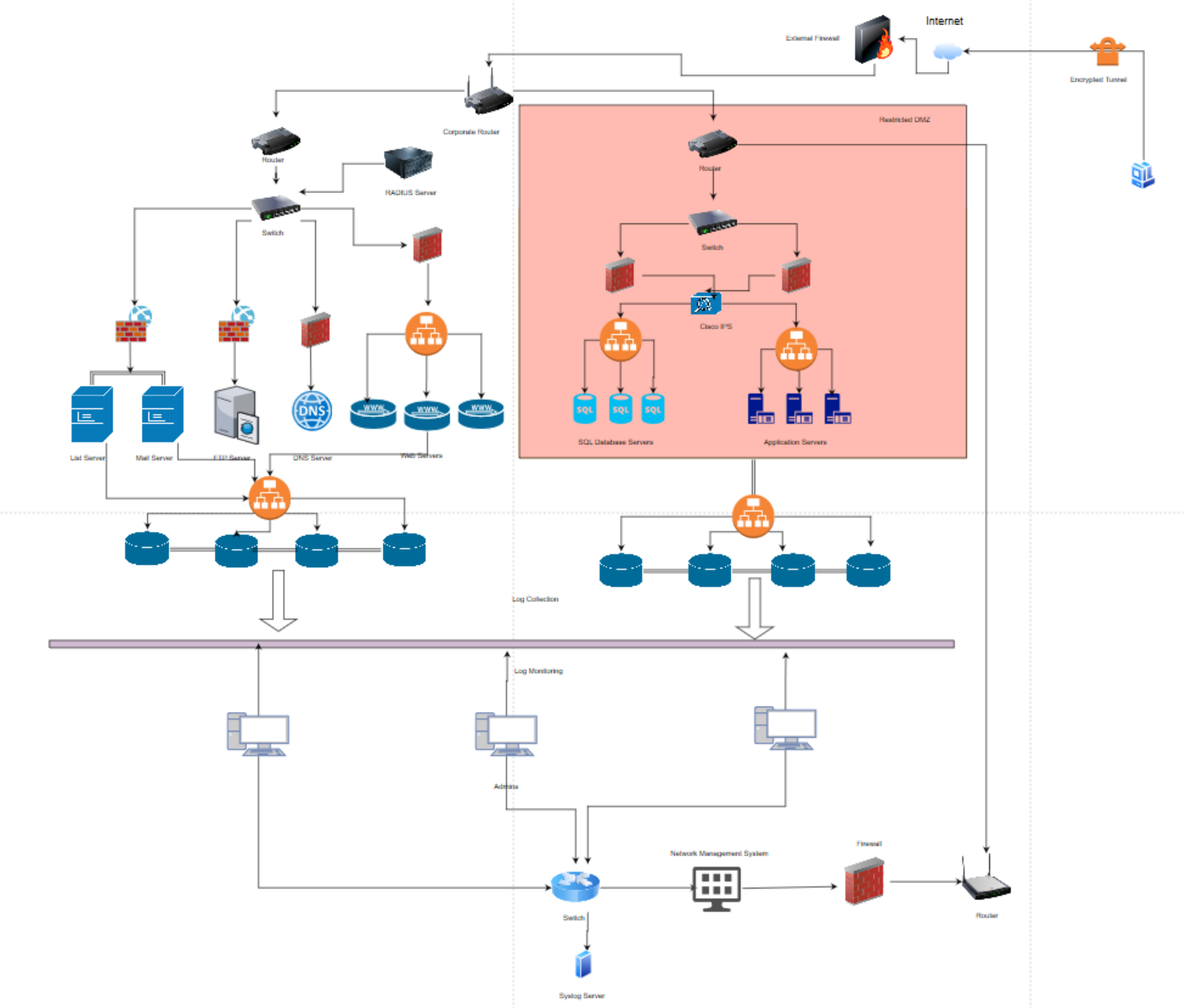
  - Logon – Rate and time limit can be applied fir the duration of logon requests which can serve as logon restrictions.
  - Production Code Change Control – There should a separation of production and development DBMS on dedicated servers.
  - Resource Control – During reassignment of data to different locations, residual risk should be cleared.
  - Audit Reduction and Report Generation – Audit Reduction and Report Generation should be automated for effective management.
  - Audit Record Retention – Audit record should also be retained for a certain period of time for analysis and investigative purposes.
  - Security Configuration Compliance – The host system, network, and other applications that depend on it needs to be secured as DBMS security also depends on it.
  - Software Development Change Controls – These development change controls are required for creation or maintenance of database objects.
  - Audit Trail Backup – Even Audit logs need to be backed-up for analysis and investigative purposes.
  - Audit Trail Protection – Audit logs contain sensitive data and needs to be stored outside the database for protection.
  - Warning Message – To help assign responsibility for database activities warning messages are used.
  - Account Control – Unauthorized access can be protected by timely removal of disabled or unused accounts.
  - Boundary Defense – Additional risk management policies are required when direct access is made to DBMS by the clients.
  - Remote Access for Privileged Functions – Malicious users can access network from a highly privileged function, hence additional risk management policies are required.

- Business Continuity
  - Protection of Backup and Restoration Assets – Physical security and information security protection policies are required for backups and restoration assets.
  - Data Backup Procedures – For maintaining availability, data backups and its data are essential.
  - Disaster and Recovery Planning – The DBMS Disaster and recovery plan should be available and tested to ensure that it works.
  - Backup Copies of Critical Software – During maintenance or security updates the applications can experience corruptions, hence backup copies of critical software are essential.
  - Trusted Recovery – Trusted recovery prevents corruption from events like system failures.

- Vulnerability and Incident Management
  - Vulnerability Management – DBMS can be compromised when timely updating or patching is not done, and incident response systems and processes are missing.

- **Create a network topology diagram for your company.**

  The Network Topology diagram stays the same as it follows defense-in-depth approach. The Network Topology diagram consists of a restricted DMZ. Here, there are several SQL database servers and Application Servers. The distribution of workloads across multiple servers is achieved by load balancers. Inside the Restricted DMZ are two stateful inspection firewalls to monitor malicious traffic. There is also a Cisco IPS to identify and block malicious activities. This is connected to a router which is in-turn connected to a corporate router. The other servers like the Mail server, FTP server, DNS Servers and Web servers are connected to packet filter firewalls. The log collection from all the servers is done by the log collectors. There are several admins to monitor and analyze the collected logs for malicious activities. A RADIUS server is implemented to authenticate remote users securely. A syslog server is also implemented for easy configuration of all logging devices.  The clients can connect through IPsec encrypted tunnel and share data securely.



- ➢ **Create a list of Cybersecurity Implementation controls that exist at your company**

- Authentication – User Accounts
    - DBMS – Database Management System is a system for managing databases and lets its users perform Data manipulation functions.
    - Application User – There can be multiple users using the database and they are allowed to perform data manipulation functions on the database.
    - DBA – There are a few database administrators in my company and each DBA manages like 25-30 DBA’s.
    - Application Account – A specialized account with elevated privileges not intended for general use and used to perform privileged functions.
    - Application Owner – There are a few application owners in my company for provisioning and de-provisioning of Application accounts.

    - Database Auditor – There also a few database auditors for auditing the different activities and also to monitor DBA's actions.
    - Database Operator – In my org, a specialized account with limited admin privileges are given for some crucial tasks like backups and database startups.
    - Passwords – 2FA is used in my company and passwords are still the primary level of authentication to the databases.
    - Certificates – PKI Certificates are used if the company undertakes any government projects.
    - External Authentication – In my company, proper authentication controls like encryption are used when authentication over the wireless network.
    - Credential Storage – For protecting credentials stored inside the database strong encryption mechanism is used and its keys are not stored in the database.

- Authorization
    - RBAC – It is the DBA's responsibility to provide users with roles and assign access controls based upon those roles.  My company uses IAM tools such as CyberArk for Identity and access management.
    - Rename default accounts – Renaming the default account names is a common practice which is also implemented at my organization for evading name-based attacks.

- Confidentiality
    - Data Encryption – In my organization, data is encrypted both at rest and in motion to ensure its confidentiality.
    - Application Code – In my organization, any application code inside the databases is encrypted to avoid being abused by malicious users.
    - Encrypt Data Files – The metadata and other data files are also encrypted.
    - Database Configuration, Transaction logs and Audit trails – This information can be abused by a sophisticated attacker hence all kinds of logs and config files are encrypted.

- Data Integrity
    - Transaction Logs – It is company policy to encrypt all transaction logs to avoid being abused by a malicious user.
    - Database Integrity – All the database regulatory compliance requirements like GDPR, SOX, GLBA, HIPPA, PCI are followed to ensure database integrity.

- Auditing
    - Audit logs Protections – All the audit logs are protected with proper encryption controls.
    - Audit logs Retention – Audit logs are retained for a period of two months in my organization.

    - Audit Reporting – All the database activities are monitored in my company and any unauthorized activities are immediately reported to the concerned DBA.

- Replication and Federation
    - Database Links – In my company, Several databases are connected together in a distributed fashion by database links.
    - Database Replication – Database replication is practiced in my company to copy any changes to the database into another database among multiple data centers.

- Backup and Recovery
    - DBMS Backup – Backup of all the data on databases is performed regularly and retained for a period of time.
    - Database Recovery – If a database becomes corrupt during security updates or patches it can be recovered to its original state.

- Operating System Protection
    - Database Directories and Files – In my company, all the Directories and files are stored on partitions on dedicated servers
    - Dedicated OS Account – Dedicated OS Accounts are used for installing any database software files.
    - Database Software – Database software is monitored for any unauthorized changes and reported to the DBA.

- Application Protection
    - Input Validation – Input validation is done in my company to check the data sent to databases are complete and accurate.
    - Review Authentication Method – In my company all authentication methods are reviewed against policies like password policy etc.
    - Minimum Privileges – In my company least privilege policy is implemented by default.

- Network Protection
    - Network Access Protection – Network Access Protection provides an additional level of protection for database security.
    - Protection against Unauthorized Disclosure – Everything which is sent or received is encrypted in my company to avoid unauthorized disclosure.

- Security Design and Configuration
    - Procedural Review – Procedural review is performed at my company to review all current database policies and procedures.
    - Configuration and Specification –configurations and specification review are done at my company to safeguard against any known threats and vulnerabilities.

  - Compliance Testing – There are several test servers at my company on which all the updates or security patches are applied to avoid corruption of actual systems.
  - Non-Repudiation – Non-Repudiation is ensured at my organization by applying strong cryptographic controls.
  - Partitioning and application – Dedicated hosts are present at my company for DBMS.
  - Ports, Protocols and Services – Network security policy guides use of secure ports, protocols and services. All the unwanted ports are blocked
  - IA Documentation –IA Risk Management Plan is readily available at my company.
  - Group Identification and Authentication – There are some group accounts which exist at my company which requires group identification and authentication policies
  - Individual Identification and Authentication – Strong identification and authentication policies are in place at my company.
  - Key Management – In my company, all the keys are stored securely outside the database.
  - Token and Certificate Standards – When handling government projects my company uses tokens like Common Access Card and PKI certificates to ensure database security.

- Enclave and Computing Environment
  - Audit Record Content – In my company, auditing of all security events is conducted regularly to detect any unauthorized activities in databases and their computing environment.
  - Audit trail, Monitoring, Analysis and Reporting – Audit trail monitoring, Analysis and Reporting is performed at my org to prevent any kind of attacks.
  - Changes to Data – Database state and data can be stored at any point from the backup stored at the company.
  - Encryption for Confidentiality: Data at Rest – Data is encrypted at rest in my company as it contains sensitive data like healthcare information, IP data, PII etc.
  - Encryption for Confidentiality: Data in Transit – Data is encrypted in transit as networks can be vulnerable to sniffing attacks.
  - Data Change Controls – Data change controls are implemented at my org so that Database recovery or rollback operation can be performed in case of incomplete or interrupted transactions.
  - Audit of Security Label Changes – Security label containing more than one category is assigned in my company to data and is a good access control mechanism.
  - Audit Reduction and Report Generation – My company uses automated tools provided by Imperva for Audit reduction and Report Generation.
  - Audit Record Retention – In my company, all the audit records are maintained for a period of 2 months

  - Audit Trail Backup – All the audit records are backed up for analysis or investigative purposes and retained for 2 months.
  - Audit Trail Protection – In my company, audit logs are encrypted as it may contain sensitive content.
  - Account Control – Regular checks are conducted at my company for disabled or unused accounts and removed immediately.

- Business Continuity
  - Protection of Backup and Restoration Assets – Imperva's Data Activity Monitoring (DAM) solutions also help in protection of backups and restoration of critical assets.
  - Data Backup Procedures – Several databases in different data centers are present for data backup procedures spread across the country.
  - Disaster and Recovery Planning – Our company has a tested and viable DBMS Disaster and recovery plan readily available.
  - Backup Copies of Critical Software – In the event of software or application corruptions my company maintains all backup copies of critical software.

- Vulnerability and Incident Management
  - Vulnerability Management – My company also uses a tool called Scuba provided by its cybersecurity vendor Imperva. It's a database vulnerability scanner which scans for vulnerabilities and misconfigurations. It also provides recommendations to mitigate the identified risks.

- **Compare the Implementation controls discussed in class with your company's existing Cybersecurity Implementation controls**

| Implementation Controls | Status |
|---|---|
| **Authentication – User Accounts** | |
| DBMS | Implemented |
| Application User | Implemented |
| DBA | Implemented |
| Application Owner | Implemented |
| Application User Manager | NOT Implemented |
| Application Account | Implemented |
| Database Auditor | Implemented |
| Database Operator | Implemented |
| Passwords | Implemented |
| Certificates | Implemented |
| External Authentication | Implemented |
| Credential Storage | Implemented |
| **Authorization** | |
| RBAC | Implemented |
| Multi-tier applications | NOT Implemented |

| | |
|---|---|
| Rename default accounts | Implemented |
| **Confidentiality** | |
| Data Encryption | Implemented |
| Application Code | Implemented |
| Encrypt Data Files | Implemented |
| Database Configuration, Transaction logs and Audit trails | Implemented |
| **Data Integrity** | |
| Transaction Logs | Implemented |
| Database Integrity | Implemented |
| **Auditing** | |
| Audit logs Protections | Implemented |
| Audit logs Retention | Implemented |
| Audit Reporting | Implemented |
| **Replication and Federation** | |
| Database Links | Implemented |
| Database Replication | Implemented |
| Federated Databases | NOT Implemented |
| **Clustering** | |
| Database Clustering | NOT Implemented |
| Accountability | NOT Implemented |
| Protect Communication Path | NOT Implemented |
| **Backup and Recovery** | |
| DBMS Backup | Implemented |
| Database Recovery | Implemented |
| **Operating System Protection** | |
| Database Directories and Files | Implemented |
| Dedicated OS Account | Implemented |
| Database Software | Implemented |
| **Application Protection** | |
| Input validation | Implemented |
| Review Authentication Method | Implemented |
| Minimum Privileges | Implemented |
| **Network Protection** | |
| Network Access Protection | Implemented |
| Time and Count limits on Network Session Parameters | NOT Implemented |
| Protection against Unauthorized Disclosure | Implemented |
| **Security Design and Configuration** | |
| Procedural Review | Implemented |
| Configuration and Specification | Implemented |
| Compliance Testing | Implemented |
| Functional Architecture for IS Applications | NOT Implemented |
| Non-Repudiation | Implemented |

| | |
|---|---|
| Partitioning and application | Implemented |
| Ports, Protocols and Services | Implemented |
| Configuration Management (CM) Process | NOT Implemented |
| IA Documentation | Implemented |
| System Library Management Controls | NOT Implemented |
| Security Support Structure Portioning | NOT Implemented |
| Software Baseline | NOT Implemented |
| Group Identification and Authentication | Implemented |
| Individual Identification and Authentication | Implemented |
| Key Management | Implemented |
| Token and Certificate Standards | Implemented |
| **Enclave and Computing Environment** | |
| Access for Need-to-know | NOT Implemented |
| Audit Record Content | Implemented |
| Audit trail, Monitoring, Analysis and Reporting | Implemented |
| Changes to Data | Implemented |
| Encryption for Confidentiality: Data at Rest | Implemented |
| Encryption for Confidentiality: Data in Transit | Implemented |
| Data Change Controls | Implemented |
| Interconnection among DoD systems and Enclaves | NOT Implemented |
| Audit of Security Label Changes | Implemented |
| Logon | NOT Implemented |
| Production Code Change Control | NOT Implemented |
| Resource Control | NOT Implemented |
| Audit Reduction and Report Generation | Implemented |
| Audit Record Retention | Implemented |
| Security Configuration Compliance | NOT Implemented |
| Software Development Change Controls | NOT Implemented |
| Audit Trail Backup | Implemented |
| Audit Trail Protection | Implemented |
| Warning Message | NOT Implemented |
| Account Control | Implemented |
| Boundary Defense | NOT Implemented |
| Remote Access for Privileged Functions | NOT Implemented |
| **Business Continuity** | |
| Protection of Backup and Restoration Assets | Implemented |
| Data Backup Procedures | Implemented |
| Disaster and Recovery Planning | Implemented |
| Backup Copies of Critical Software | Implemented |
| Trusted Recovery | NOT Implemented |
| **Vulnerability and Incident Management** | |
| Vulnerability Management | Implemented |

- **Create a list of critical assets in $ that exist in your company**

Data is the most important asset at our company.
Some of the critical assets are:
Patients health records: Maintaining Patients health records is crucial to our organization. It will cost millions if there is any breach involving patient’s health records.

Client Information: Doctors and patient’s information are one of the crucial assets. Damage control will cost millions if there are any data leaks.

Employee Information: It consists of HR records. Damage control and credit monitoring services would cost the company millions of dollars of there is a breach.

Organization Reputation: Positive Reputation for a corporation is essential for building trust and is one of the critical assets. It is intangible.

Network Devices: There are numerous network devices which could be categorized as critical assets. As Data is the most important asset, servers like SQL database are the most critical assets at our organization. Other important assets include Servers, firewalls, routers, Cisco IPS etc. These network devices cost hundreds of thousands of dollars.

| S. No | Asset | Value (Approx.) |
|---|---|---|
| 1 | Patient Health Records | $200 Million |
| 2 | Client Information | $100 Million |
| 3 | Employee Information | $10 Million |
| 4 | Organization Reputation | Intangible |
| 5 | Network Devices | $5 Million |

- **Create a list of potential vulnerabilities for critical assets where Cybersecurity Implementation Controls are missing**

  - The Time and Count limits on Network session parameters is not implemented in my organization. The most common time limit set for sessions in 10 min although Web Admins usually set it for 8 min.
  - Federated databases and database Clustering are not implemented at my company. They improve data distribution across multiple databases.
  - As configuration management practices are not followed it would be difficult to recover from malicious attacks. It also leads to more efficient change management.
  - Due to missing Security Support Structure Positioning, it is easy for malicious users to access the security policies.

- Boundary defense is not implemented in my company and thus be vulnerability to many network related attacks.

- **Create a list of potential threats to your company that could exploit vulnerabilities of critical assets.**

  - In the event of a DOS attack, the recovery might be difficult due to the missing of clustering and federation features like load balancing, high availability support thereby increasing downtime costing the company thousands of dollars.
  - In the absence of security support structure positioning, malicious user may change the security policies which may result in a whole range of compliance issues.
  - As Time and Count limits on Network session parameters is not implemented, several malicious attacks like session hijacking could be possible.
  - DOS attacks and malware can spread on the internal network as boundary defenses are not implemented.

- **Create a list of potential risks for critical assets where Cybersecurity Implementation Controls are missing**

  - Denial of Service: DOS attacks are a possibility due to the absence of boundary defenses and recovery can be difficult due to missing controls like clustering and federation. This can have a high impact as providing services to the organization is paramount.
  - Unauthorized access: Due to the absence of security support structure positioning, and boundary defenses, malware can spread through the internal network and unauthorized access is a possibility.
  - Disclosure of sensitive information: Attacks like Session hijacking can lead to stealing and disclosure of sensitive information.
  - Data confidentiality, Integrity and Authenticity can be compromised as general users can access the security policies of an organization.

- **Provide a list of recommended Hardening Prevention controls and policies for each recommended control that should be created to reduce vulnerability probabilities and thus mitigate the identified risks (it is not required to write detailed policies) – Risk Prevention Strategy.**

  - Implementing Time and Count limits on Network session parameters can greatly increase the security of the database while prevent many malicious attack attempts.

- Boundary defense needs to be implemented which acts like a first line of defense to safeguard sensitive information and keep the malicious traffic out from the internal network.
- Warning messages can also be implemented to detect any malicious attempts.
- security support structure positioning should be implemented to ascertain the security policies are safeguarded from malicious users.

➢ **Provide a list of recommended Hardening methods and policies for critical assets that should be implemented to reduce asset risk impact and thus mitigate the identified risks and increase resilience (it is not required to write detailed policies) – Risk Response Strategy**

- It is good to implement clustering and federated databases to recover quickly against DOS attacks and reduce downtime.
- Following good configuration management practices, the visibility, performance, and efficiency can be increased deterring data breaches and reducing the risk of outages.
- In the event of system failures and corruptions trusted recovery can help recover thus promoting business continuity.

➢ **Create a detailed policy for the Database Credentials Coding control using a SANS template as provided in class**

# Database Credentials Coding Policy

**Free Use Disclaimer:** *This policy was created by or for the SANS Institute for the Internet community. All or parts of this policy can be freely used for your organization. There is no prior approval required. If you would like to contribute a new policy or updated version of this policy, please send email to policy-resources@sans.org.*

**Last Update Status:** *Updated June 2014*

## 1. Overview

Database authentication credentials are a necessary part of authorizing application to connect to internal databases. However, incorrect use, storage and transmission of such credentials could lead to compromise of very sensitive assets and be a springboard to wider compromise within the organization.

## 2. Purpose

This policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of company's networks.

Software applications running on company's networks may require access to one of the many internal database servers. To access these databases, a program must authenticate to the database by presenting acceptable credentials. If the credentials are improperly stored, the credentials may be compromised leading to a compromise of the database.

## 3. Scope

This policy is directed at all system implementer and/or software engineers who may be coding applications that will access a production database server on the company Network. This policy applies to all software (programs, modules, libraries or APIS that will access a company, multi-user production database. It is recommended that similar requirements be in place for non-production servers and lap environments since they do not always use sanitized information.

## 4. Policy

General

To maintain the security of company's internal databases, access by software programs must be granted only after authentication with credentials. The credentials used for this authentication must not reside in the main, executing body of the program's source code in clear text. Database credentials must not be stored in a location that can be accessed through a web server.

Specific Requirements

Storage of Data Base Usernames and Passwords

- Database usernames and passwords may be stored in a file separate from the executing body of the program's code. This file must not be world readable or writeable.

- Database credentials may reside on the database server. In this case, a hash function number identifying the credentials may be stored in the executing body of the program's code.

- Database credentials may be stored as part of an authentication server (i.e., an entitlement directory), such as an LDAP server used for user authentication. Database authentication may occur on behalf of a program as part of the user authentication process at the authentication server. In this case, there is no need for programmatic use of database credentials.

- Database credentials may not reside in the documents tree of a web server.

- Pass through authentication (i.e., Oracle OPS$ authentication) must not allow access to the database based solely upon a remote user's authentication on the remote host.

- Passwords or pass phrases used to access a database must adhere to the Password Policy.

Retrieval of Database Usernames and Passwords

- If stored in a file that is not source code, then database usernames and passwords must be read from the file immediately prior to use. Immediately following database authentication, the memory containing the username and password must be released or cleared.

- The scope into which you may store database credentials must be physically separated from the other areas of your code, e.g., the credentials must be in a separate source file. The file that contains the credentials must contain no other code but the credentials (i.e., the username and password) and any functions, routines, or methods that will be used to access the credentials.

- For languages that execute from source code, the credentials' source file must not reside in the same browsable or executable file directory tree in which the executing body of code resides.

Access to Database Usernames and Passwords

- Every program or every collection of programs implementing a single business function must have unique database credentials. Sharing of credentials between programs is not allowed.

- Database passwords used by programs are system-level passwords as defined by the Password Policy.

- Developer groups must have a process in place to ensure that database passwords are controlled and changed in accordance with the Password Policy. This process must include a method for restricting knowledge of database passwords to a need-to-know basis.

Coding Techniques for implementing this policy

[Add references to your site-specific guidelines for the different coding languages such as

Perl, JAVA, C and/or Cpro.]

## 5. Policy Compliance

### 5.1. Compliance Measurement

The Infosec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

### 5.1. Exceptions

Any exception to the policy must be approved by the Infosec team in advance.

### 5.2. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

A violation of this policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with company.

Any program code or application that is found to violate this policy must be remediated within a 90-day period.

## 6. Related Standards, Policies and Processes

- Password Policy

## 7. Definitions and Terms

- Credentials
- Executing Body
- Hash Function
- LDAP
- Module

## 8. Revision History

| **Date of Change** | **Responsible** | **Summary of Change** |
|---|---|---|
| June 2014 | SANS Policy Team | Formatted into new template and made minor wording changes. |
| | | |

| **Version** | **Revision Date** | **Author** |
|---|---|---|
| V1.0 | 11/10/2019 | Abhishek Ningala |