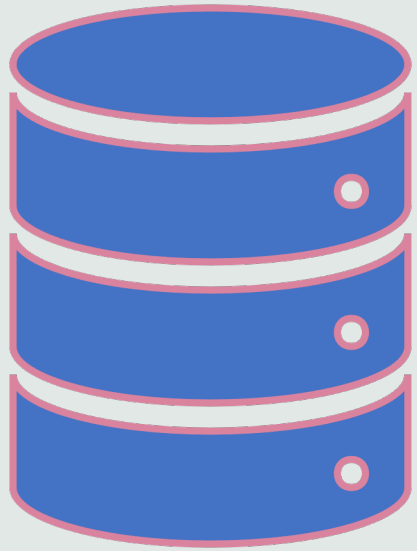
ITMD 321 Group Project

By Greg Eure, Muhammed Zahid, Calvin Ton, Junyan Liu, Estefania Lopez

Database Specifications



DATABASE SPECIFICATIONS

Group Presentation and Project,

- Greg Eure, Muhammed Zahid, Calvin Ton, Junyan Liu, Estefania Lopez

ITMD 321: Data Modeling and Applications

Dr. Maurice Dawson

November, 2020

Revision Sheet

Release No.	Date	Revision Description
Rev. 1	11/27/20	Initial publication of specifications

Database Specifications Authorization Memorandum

I have carefully assessed the Database Specifications for the Global Terrorism Database (GTD). This document has been completed in accordance with the requirements of the HUD System Development Methodology.

MANAGEMENT CERTIFICATION - Please check the appropriate statement.

___X__ The document is accepted.

_____ The document is not accepted.

We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.

_Greg Eure_____ _11/27/2020_____
NAME DATE
Project Leader

_Muhammed Zahid_____ _11/27/2020_____
NAME DATE
Operations Division Director

_Calvin Ton_____ _11/27/2020_____
NAME DATE
Program Area/Sponsor Representative

_Junyan Liu_____ _11/27/2020_____
NAME DATE
Program Area/Sponsor Director

_Estefania Lopez_____ _11/27/2020_____
NAME DATE
Program Area/Sponsor Controller

DATABASE SPECIFICATIONS

TABLE OF CONTENTS

1.0 GENERAL INFORMATION

1.0 GENERAL INFORMATION

1.1 Purpose

The purpose of the Database Specifications is to provide database architecture, design, configuration, controls, and administrative information for primary stakeholders, IT development, and database support personnel.

1.2 Scope

The scope of the Database Specifications as it relates to the ITMD 321 Group Presentation and Project are:

- Describe database architecture & design
- Describe database administrative information
- Describe database security controls

1.3 System Overview

The GTD is a database downloaded from the National Consortium for the Study of Terrorism and Responses to Terrorism. It serves as a sample database for the ITMD 321 group project to demonstrate effective database documentation and security control practices.

- Responsible organization: ITMD 321 group members Greg Eure, Muhammed Zahid, Calvin Ton, Junyan Liu, Estefania Lopez
- System name: GroupProj
- System code: Github link: https://github.com/SQLGROUPPROJ/SQLPROJ
- System Category: general support system - provides general database functionality to demonstrate documentation and security controls
- Operational status: Operational
- System environment: any operating system running MySQL

1.4 Project References

The below references were used in preparation for this document:

- Group Presentation and Project Assignment Guidance document
- Database Security Project Guidance sample document
- HUD Database Specifications 15145 document

1.5 Acronyms and Abbreviations

- GTD: Global Terrorism Database
- ITMD: Information Technology & Management & Development

- POC: Points of Organizational Contact
- HUD: Housing and Urban Development
- DBMS: Database Management System
- QA: Quality Assurance
- SQL: Structured Query Language

1.6 Points of Contact

1.6.1 Information

List of POCs for informational and troubleshooting purposes:

- Architecture POC: Greg Eure, email: geure@hawk.iit.edu
- Infrastructure POC: Muhammed Zahid, email: mzahid3@hawk.iit.edu
- Helpdesk POC: Calvin Ton, email: cton@hawk.iit.edu
- Development POC: Junyan Liu, email: jliu192@hawk.iit.edu
- Operations POC: Estefania Lopez, email: elopez17@hawk.iit.edu

1.6.2 Coordination

List of organizations that require coordination between the project and its specific support function:

- (Hardware Team) Server Procurement (on-premise or cloud provisioning, includes server and data storage): Schedule: week 1
- (Server Team) Operating System Installation and Configuration: Schedule: week 2
- (DBMS Team) DBMS Installation and Configuration: Schedule: week 3
- (DBMS Team) Database GTD Installation and Configuration: Schedule: week 4
- (Development Team) Database testing: Schedule: week 5
- (Security Team) Database security checking and system audit: week 6
- (QA Team) Rigorous system testing and sign-off: week 7

1.6.3 Additional Points of Contact

Additional points of contact are included in section 3.1.

1.6.4 Data Owners

See section 1.6.1.

2.0 DATABASE IDENTIFICATION AND DESCRIPTION

2.0 DATABASE IDENTIFICATION AND DESCRIPTION

2.1 Naming Conventions

Discuss the logical and physical naming standards and conventions.

2.2 Database Identification

Identify the names or labels by which the database may be uniquely identified. Specify the code name, tag, or label by which each database table or file may be uniquely identified.

Database name:

- GroupProj

Tables:

- Afghanistan
- Albania
- Algeria
- Angola
- Argentina
- Armenia
- Australia
- Austria
- Azerbaijan
- Bahrain
- Bangladesh
- Belgium
- Bolivia
- Brazil
- Bulgaria
- BurkinaFaso
- Burundi
- Cameroon
- Canada
- Chili
- Incidents

2.3 Systems Using the Database

No other systems will use the GroupProj database. This is a demonstration database only, as documented in this guide.

2.4 Relationship to Other Databases

The GroupProj database will not supersede or interface with other databases.

2.5 Schema Information

Describe the overall structure in the schema or other global definition of the database.

The GropProj is a schema which holds the information of terror attacks that happened between 2016 to 2018. There are a total of 21 tables in the schema, 20 of those tables correspond to a different country and contain 33 attributes listing information such as motive, attack type, weapons used and other pieces of useful information regarding terror attacks. The remaining table is a collection of all incidents and contains 2 attributes, incident_id and test_id.

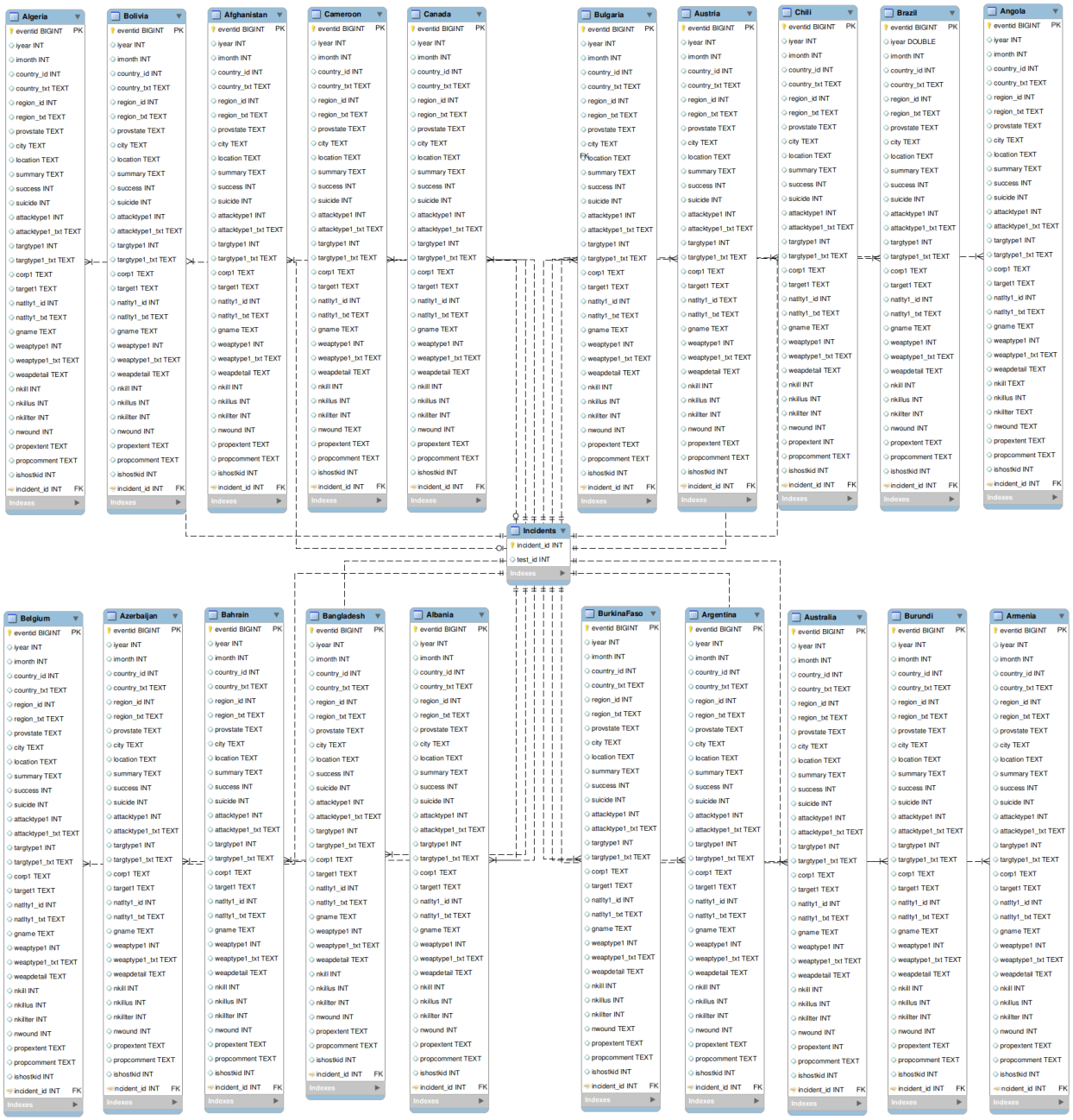
2.5.1 Description

Describe the schema and each sub-schema of the system including name, file type and name, data description language, access control keys, concurrence locking, data name mapping, overall partition/file limitations and controls, redefinition and access path restrictions and any other limitations or restrictions.

The GroupProj schema was used to design our system. Our system connects all tables using the ‘incidence’ tables on incident_id. In order to create our system we used DDL commands such as CREATE, DROP and ALTER. Our system has 4 distinct roles: administrator, end user, client and testing.
The schema GroupProj doesn’t have any sub-schema

2.5.2 Physical Design

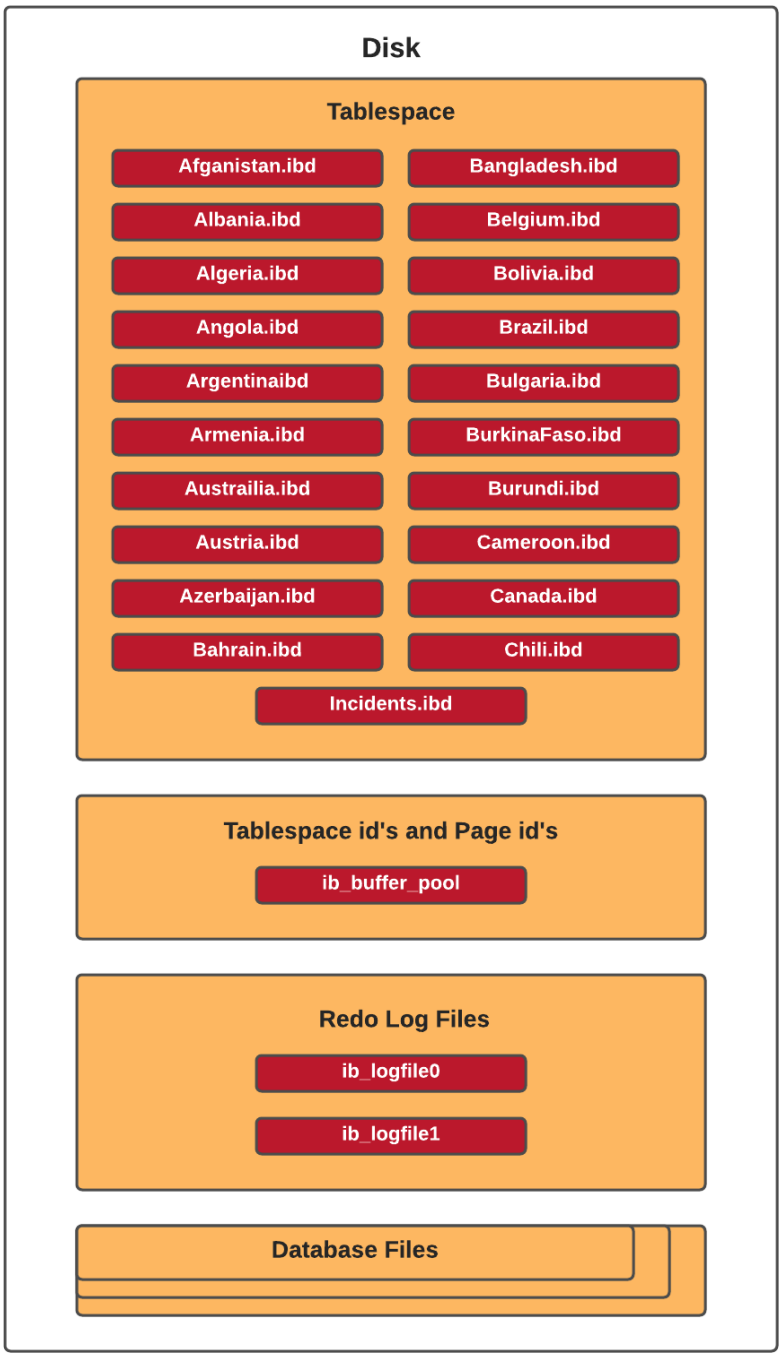
Graphically depict the physical design of the database.



2.5.3 Physical Structure

Describe and depict in a graphic representation the physical structure (partitions, files, indexes, pointers) and the logical components of the database. Identify the criteria required to achieve operating efficiency.

The DBMS resides on the filesystem in the /var/lib/mysql directory. The database resides on the filesystem in the /var/lib/mysql/GroupProj directory. There are no partitions or pointers. There are at least 3 indexes per table, consisting of the primary key index, the foreign key index, and an eventid index.



2.6 Data Dictionary

Reference the data dictionary and attach it as an appendix to this document.

	Field Name	Data Type	Description
2	eventid	BIGINT	Event Id Auto incremented
3	iyear	INT	Year event took place in
4	imonth	INT	Month event took place in
5	country_id	INT	Country id event took place in
6	country_txt	TEXT	Country Name event took place in
7	region_id	INT	Region Id where event took place in
8	region_txt	TEXT	Region text where event took place in
9	provstate	TEXT	State where event took place in
10	city	TEXT	City Where event took place in
11	location	TEXT	Exact Location of the event
12	summary	TEXT	summary of the event
13	success	INT	Was it successful
14	suicide	INT	any sucide
15	attacktype1	INT	what type of attach
16	attacktype1_tx	TEXT	exaplaning what type of attach
17	targtype1	INT	Who was the target
18	targtype1_txt	TEXT	exaplaning the target
19	corp1	TEXT	Corp who handled the event
20	target1	TEXT	who was the target
21	natity1_id	INT	Nationality ID
22	natity1_txt	TEXT	Nationality Text
23	gname	TEXT	Org Name
24	weaptype1	INT	Weapon type id
25	weaptype1_txt	TEXT	Weapon type text
26	weapdetail	TEXT	Explaining the weapon
27	nkill	INT	no killed in the event
28	nkillus	INT	no killer
29	nkilter	INT	no of the kill
30	nowound	INT	no wounded
31	propextent	TEXT	property damage
32	propcomment	TEXT	property damage explaining
33	ishostkid	INT	is the host kid
34	incident_id	INT	incident id

2.7 Special Instructions

Identify instructions to be followed by personnel who will contribute to the generation of the database and who will use it for testing and operational purposes. Such instructions may include:

There are no specific instructions

3.0 DATABASE ADMINISTRATIVE INFORMATION

3.0 DATABASE ADMINISTRATIVE INFORMATION

3.1 Responsibility

Identify the organizations and personnel responsible for the following database administrative functions: database administrator, system administrator, and security administrator. Describe specific administration skill requirements.

Database administrator organization: DBMS Services
DBMS Services responsible personnel: Muhammed Zahid
Database administrator required skills:

- Knowledge of database queries
- Knowledge of database theory
- Knowledge of database design
- Knowledge about the RDBMS itself, e.g. Microsoft SQL Server or MySQL
- Knowledge of structured query language (SQL), e.g. SQL/PSM or Transact-SQL
- General understanding of distributed computing architectures, e.g. Client–server model
- General understanding of operating system, e.g. Windows or Linux
- General understanding of storage technologies and networking
- General understanding of routine maintenance, recovery, and handling failover of a database

System Administrator organization: Operations Services
Operations Services responsible personnel: Estefania Lopez
System Administrator required skills:

- Problem-Solving and Administration
- Networking
- Cloud
- Automation and Scripting, including HTML, JavaScript, Go, Bash, Python, and Node.js
- Security and Monitoring
- Account Access Management
- IoT/Mobile Device Management
- Hardware Management
- SQL

Security Administrator organization: Security Management

Security Management responsible personnel: Calvin Ton

Security Administrator required skills:

- Defending systems against unauthorized access, modification and/or destruction
- Scanning and assessing network for vulnerabilities
- Monitoring network traffic for unusual activity

- Configuring and supporting security tools such as firewalls, anti-virus software and patch management systems
- Implementing network security policies, application security, access control and corporate data safeguards
- Training fellow employees in security awareness and procedures
- Developing and updating business continuity and disaster recovery protocols

3.2 System Information

Document the Database Management System configuration, hardware configuration, database software utilities, and any support software used:

DMBS configuration: MySQL Server installation on test environment with mysql_secure_installation script execution
Hardware configuration: Test environment running on virtual machine with 2 cpu's, 4Gb RAM, and 32Gb disk, with Ubuntu linux installed
Database software utilities: MySQL Workbench installed on test environment

3.2.1 Database Management System (DBMS) Configuration

Identify the vendor, version or release date and targeted hardware for the DBMS. Describe any restrictions on the initialization and use of the DBMS to support any intended distributed processing.

The targeted hardware can be any x86-based commodity hardware, including dedicated or virtualized environments. No restrictions are identified.

3.2.2 Hardware Configuration

Identify the hardware configurations on which the database will reside.

No strict hardware configurations are required, but the test system is running 2 vcpu's, 4 Gb memory, and 32 Gb disk.

3.2.3 Database Software Utilities

List and reference the documentation of any DBMS utility software available to support the use or maintenance of the database.

DBMS support: https://dev.mysql.com/doc/
MySQL Workbench support: https://dev.mysql.com/doc/workbench/en/wb-intro.html

3.2.4 Support Software Available for Maintaining Database

Describe all support software, including the operating system, directly related to the database, including name, version, function, and major operating characteristics. Cite documentation by title, number, and appropriate sections. Examples of such software include database management systems, query language, report writers, storage allocation software, database loading software programs, and file processing programs, and data cleaning software.

Operating System: Ubuntu, version 20.04.01 LTS, function: database server
DBMS System: MySQL Community Server, version 8.0.22, function: DBMS server
Tool: MySQL Workbench, version 8.0.22, function: MySQL support tool
Query Language: structured query language (SQL)

3.2.5 Security

Describe the use and management of integrity and access controls that apply to all database components such as schema, sub-schema, partitions or physical files, records or tables, sets or relations, and data elements.

The database shall be secured initially by executing the mysql_secure_installation script provided by MySQL. Additionally, the following roles shall be granted as specified to database GroupProj:

- database_administrator
- user
- client
- testing

These roles may be created by executing these sql commands:

```
CREATE ROLE database_administrator;
CREATE USER 'GlobalProj_admin'@'localhost' IDENTIFIED BY '<password>';
GRANT SELECT, INSERT, UPDATE, DELETE ON globalproj.* TO database_administrator;
GRANT database_administrator TO 'GlobalProj_admin'@'localhost';
CREATE ROLE end_user;
CREATE USER 'GlobalProj_user'@'localhost' IDENTIFIED BY '<password>';
GRANT end_user TO 'GlobalProj_user'@'localhost';
GRANT SELECT, INSERT, UPDATE ON globalproj.* TO end_user;
CREATE ROLE client;
CREATE USER 'GlobalProj_client'@'localhost' IDENTIFIED BY '<password>';
GRANT client TO 'GlobalProj_client'@'localhost';
GRANT SELECT ON globalproj.* TO client;
CREATE ROLE testing;
CREATE USER 'GlobalProj_testing'@'localhost' IDENTIFIED BY '<password>';
GRANT SELECT, UPDATE ON globalproj.* TO testing;
GRANT testing TO 'GlobalProj_testing'@'localhost';
```

*** where <password> is the actual password ***

The database instance shall also be secured in a manner consistent and compliant with NIST 800-53. All relevant controls shall be documented in separate control documents (defined below), along with respective test case results.

NIST 800-53 Control Description		
Control Number	**Control Description**	**Control Enforcement Procedure**

AC-7	Unsuccessful Login Attempts	NIST AC-7 Control Document
AU-2	Audit Events	NIST AU-2 Control Document
CM-10	Software Usage Restrictions	NIST CM-10 Control Document
IA-6	Authenticator Feedback	NIST IA-6 Control Document
SA-2	Allocation of Resources	NIST SA-2 Control Document
SC-5	Denial of Service Protection	NIST SC-5 Control Document
SI-3	Malicious Code Protection	NIST SI-3 Control Document
AC-2	Account Management	NIST AC-2 Control Document
AC-5	Separation of Duties	NIST AC-5 Control Document
AT-3	Role-Based Security Training	NIST AT-3 Control Document
AU-3	Content of Audit Records	NIST AU-3 Control Document
CM-6	Configuration Settings	NIST CM-6 Control Document
AU-8	Session Audit	NIST AU-8 Control Document
AC-8	System Use Notification	NIST AC-8 Control Document
PE-15	Water Damage Protection	NIST PE-15 Control Document
CA-5	Plan of Action and Milestones	NIST CA-5 Control Document
CP-9	Information System Backup	NIST CP-9 Control Document
CP-10	Information System Recover & Reconstitution	NIST CP-10 Control Document

CM-2	Baseline Configuration	NIST CM-2 Control Document
MP-2	Media Access	NIST MP-2 Control Document
PE-8	Visitor Access Records	NIST PE-8 Control Document
AC-14	Permitted Actions Without Identification or Authentication	NIST AC-14 Control Document
AC-17	Remote Access	NIST AC-17 Control Document
AC-22	Publicly Accessible Content	NIST AC-22 Control Document
SA-3	System Development Life Cycle	NIST SA-3 Control Document
IR-4	Incident Handling	NIST IR-4 Control Document
SC-7	Boundary Protection	NIST SC-7 Control Document
AC-3	Access Enforcement	NIST AC-3 Control Document
AC-20	Use of External Information System	NIST AC-20 Control Document
AT-4	Security Training Record	NIST AT-4 Control Document
CM-11	User-Installed Software	NIST CM-11 Control Document
IR-5	Incident Monitoring	NIST IR-5 Control Document
PS-7	Third-Party Personnel Security	NIST PS-7 Control Document
PS-6	Access Agreements	NIST PS-6 Control Document
PL-4	Rules of Behavior	NIST PL-4 Control Document
PE-13	Fire Protection	NIST PE-13 Control Document

3.3 Storage Requirements

Describe the storage device. Provide sizing formulas for determining the storage required to support the database content and associated software. Estimate the internal and peripheral storage requirements. Identify multiple storage requirements for distributed processing.

The storage device can be any internal or external storage that is recognized and mounted by the operating system. Minimum recommended storage for the operating system is 10 Gb. Minimum required storage for installation of MySQL is 300 Mb (minimum recommended is 1 Gb). Minimum required storage for the GroupProj database is 15Mb. For distributed processing, multiply these requirements by the number of servers to be added to the resource cluster.

3.4 Recovery

Describe the methodology for reestablishment or recreation of the necessary data schema and system support files.

Regular system back-ups are recommended, in which case system restore will be an option for complete recovery. Optionally, database exports should be performed as a secondary back-up option. Full database exports should be performed within MySQL Server or MySQL Workbench, and kept on a separate and independent system. In case recreation of the database is necessary, a fresh installation of MySQL Community Server and MySQL Workbench can be performed, followed by importing the latest export of the GroupProj database.

3.5 Partition/File Information

3.5.1 Content

Describe the content of each partition/file, listing the records it contains and explaining the purpose.

The GroupProj database is not partitioned. The database is contained under the file directory /var/lib/mysql/GroupProj. Files in this directory are associated with the defined tables in the database:

- Afghanistan.ibd
- Albania.ibd
- Algeria.ibd
- Angola.ibd
- Argentina.ibd
- Armenia.ibd
- Australia.ibd
- Austria.ibd
- Azerbaijan.ibd
- Bahrain.ibd
- Bangladesh.ibd
- Belgium.ibd
- Bolivia.ibd

- Brazil.ibd
- Bulgaria.ibd
- BurkinaFaso.ibd
- Burundi.ibd
- Cameroon.ibd
- Canada.ibd
- Chili.ibd
- Incidents.ibd

3.5.2 Description

Describe the design and format of each partition/file, including name, type, code, mapping, limitations and controls, access procedures, and mechanisms.

The file names are listed in section 3.5.1. There is no unique type, code, mapping, limitation, or mechanism. All controls and access procedures are handled by the operating system (for file/directory access) or MySQL (for database, table, data access)

3.5.3 Partition/File Interdependencies

Identify the interdependencies of each partition/file in the database.

All identified files (as listed in section 3.5.1) are dependent on file incidents.ibd, as all other tables have foreign key relationships with the primary key in this file. See section 2 for detailed database architecture.

3.6 Database Interfaces

Provide a description of the interfaces with other application software including these of other operational capabilities and from other organizations. For each interface, specify the following information:

The GlobalProj database doesn't have any interfaces with other application software not defined in this document.

3.6.1 Description of Operational Implications

Describe operational implications of data transfer, including security considerations.

N/A

3.6.2 Description of Data Transfer Requirements

Describe data transfer requirements to and from the software, including data content, format, sequence, and any conversion issues.

N/A

3.6.3 Description of Formats of Data

Describe formats of data for both the sending and receiving systems, including the data item names, codes, or abbreviations that are to be interchanged, as well as any units of measure/conversion issues.

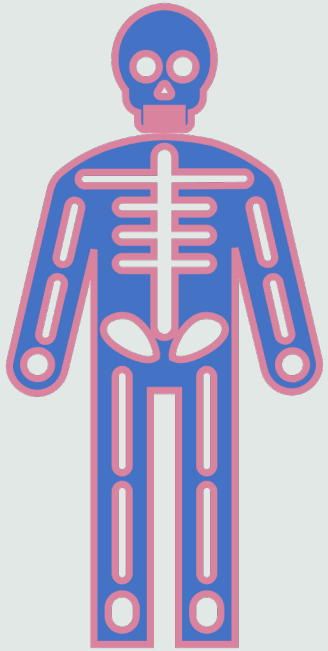
N/A

3.7 Error Handling

Describe those system error handling routines and procedures that are available during execution of database software.

Error handling is performed inherently by the MySQL DBMS software. No custom or proprietary error handling routines or procedures are implemented.

NIST 800-53 Control Documents



MySQL Unsuccessful Logon Attempts Control Policy (NIST AC-7)

1. MySQL Unsuccessful Logon Attempts Configuration (next section) shall be implemented for each identified target system.

2. A limit of 3 consecutive invalid logon attempts will be enforced.

3. The account will be automatically locked for a period of 1 day when the maximum number of unsuccessful logon attempts is exceeded.

MySQL Unsuccessful Logon Attempts Configuration (NIST AC-7)

1. In a connected and logged-in mysql prompt, run the following, where <user> is the actual name of the user account, and <password> is the actual password:

   ```
   CREATE USER <user>@localhost IDENTIFIED BY '<password>'
   FAILED_LOGIN_ATTEMPTS 3 PASSWORD_LOCK_TIME 1;
   ```

   Expected response:

   ```
   Query OK, 0 rows affected (0.02 sec)
   ```

2. Existing users can be altered by running the following, where <user> is the actual name of the user account:

   ```
   ALTER USER <user>@localhost FAILED_LOGIN_ATTEMPTS 3
   PASSWORD_LOCK_TIME 1;
   ```

   Expected response:

   ```
   Query OK, 0 rows affected (0.02 sec)
   ```

MySQL Audit Control Policy (NIST AU-2)

1. MySQL Audit Function Install/Configure (next section) shall be implemented for each identified target system.

2. All events will be audited (logged) for each occurrence of the event.

3. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events.

4. Auditable events are deemed to be adequate to support after-the-fact investigations of security incidents since each and every event is logged.

5. All events shall be enabled as being audited and logged. Audit logs shall be reviewed once per week by the security operations team. Any event which requires investigation shall kick-off an audit log review by the aforementioned team.

MySQL Audit Function Install/Configure (NIST AU-2)

6. Copy audit_log.so to /usr/lib/mysql/plugin

7. In a connected and logged-in mysql prompt, run the following:
   ```
   install plugin audit_log soname 'audit_log.so';
   ```

   Expected response:
   ```
   Query OK, 0 rows affected (0.03 sec)
   ```

8. In a connected and logged-in mysql prompt, run the following:
   ```
   Show plugins;
   ```

   Expected response (near the bottom):
   ```
   | audit_log | ACTIVE | AUDIT | audit_log.so | GPL |
   46 rows in set (0.00 sec)
   ```

9. Add the below line to /etc/mysql/mysql.conf.d/mysql.cnf and save the file:
   ```
   audit_log_file = /var/log/mysql/audit.log
   ```

10. Restart MySQL:
    ```
    sudo systemctl restart mysql
    ```

11. In a connected and logged-in mysql prompt, run the following:
    ```
    mysql> show global variables like 'audit%';
    ```

    Expected result (or similar):
    ```
    +--------------------------+-------------------------+
    | Variable_name            | Value                   |
    +--------------------------+-------------------------+
    | audit_log_buffer_size    | 1048576                 |
    | audit_log_file           | /var/log/mysql/audit.log |
    ```

```
| audit_log_flush            | OFF                      |
| audit_log_format           | OLD                      |
| audit_log_handler          | FILE                     |
| audit_log_policy           | ALL                      |
| audit_log_rotate_on_size   | 0                        |
| audit_log_rotations        | 0                        |
| audit_log_strategy         | ASYNCHRONOUS             |
| audit_log_syslog_facility | LOG_USER                 |
| audit_log_syslog_ident     | percona-audit            |
| audit_log_syslog_priority | LOG_INFO                 |
+----------------------------+--------------------------+
12 rows in set (0.00 sec)
```

12. Connect to the database and perform a query to test the audit.log function:

```
mysql> use GroupProj;
Database changed
mysql>select * from GroupProj.Angola;
------------------------
7 rows in set (0.00 sec)
```

13. Check /var/log/mysql/audit.log for capture:

```
# sudo cat /var/log/mysql/audit.log
```

Result:

```
<AUDIT_RECORD
  NAME="Query"
  RECORD="69_2020-11-21T01:59:59"
  TIMESTAMP="2020-11-21T02:12:05Z"
  COMMAND_CLASS="select"
  CONNECTION_ID="8"
  STATUS="0"
  SQLTEXT="select * from GroupProj.Angola"
  USER="root[root] @ localhost []"
  HOST="localhost"
  OS_USER=""
  IP=""
  DB=""
/>
```

Software Usage Restrictions (NIST CM-10)

1. Software and associated documentation shall be used in accordance with contract agreements and copyright laws.
2. Software and associated documentation is manually tracked via software inventory, and is protected by tracking quantity licenses to control copying and distribution.
3. Peer-to-peer file sharing shall be restricted to specific roles which are required for identified business processes. Only authorized personnel and user roles shall utilize peer-to-peer file sharing for the purpose of performing identified business functions. The use of peer-to-peer file sharing is documented and controlled to ensure that it is not used for unauthorized distribution, display, performance, or reproduction of copyrighted work.
4. The installation of Open Source Software is restricted to software which must:
    a. Be legally licensed
    b. Adhere to the secure configuration baseline

Software Inventory

Vendor	Product	Version	License	Server Count
Ubuntu	Desktop	20.04.01 LTS	GNU General Public License	1
Oracle	MySQL Community Server	8.0.22	GNU General Public License	1
Oracle	MySQL Workbench	8.0.22	GNU General Public License	1

Peer-to-Peer Tracking

Server	Technology	User or Role	Reason
none	none	none	n/a

Authenticator Feedback (NIST IA-6)

1. The information system shall obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.

2. MySQL versions 8 and higher inherently obscure feedback of authentication information.

3. MySQL Workbench versions 8 and higher inherently obscure feedback of authentication information.

4. Ubuntu Desktop versions 20 and higher inherently obscure feedback of authentication information.

Allocation of Resources (NIST SA-2)

1. The CIO is responsible for budgeting and capital planning for information technology, which will include allocating proper resources for information security.
2. The information security officer will prepare request for new services or products based on risk management decisions and forward them to the CIO for consideration and review.
3. The information security officer shall determine information security requirements for the information system or information system service in mission/business process planning.

Denial of Service Protection (NIST SC-5)

1. Network edge security devices (Unified Threat Management (UTM) or next generation firewalls (NGFW)) shall be employed to protect information system components on internal organizational networks from being directly affected by denial of service attacks.
2. Database shall be employed on a server cluster such that denial of service attacks are mitigated.
3. Appropriate network, access control lists, IPS controls, and proactive monitoring shall be implemented to decrease risk of denial of service attacks (internal and external) on critical systems.

Malicious Code Protection (NIST SI-3)

1. ClamAV shall be deployed on database server (next section) to detect and eradicate malicious code.
2. ClamAV shall be updated whenever new releases are available.
3. ClamAV shall be configured to:
    a. Perform daily scans of the server and real-time scans of files from external sources as the files are downloaded, opened, or executed
    b. Block and quarantine malicious code and sends alert to administrator in response to malicious code detection
    c. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

ClamAV Installation and Configuration (NIST SI-3)

Implement the following steps on a terminal console for the desired database server:

1. sudo apt-get update

2. sudo apt-get -y install clamav-daemon

3. sudo systemctl enable clamav-daemon

4. sudo systemctl start clamav-daemon

5. $ tail /var/log/clamav/clamav.log

   Response:
   ```
   Sun Jun 28 19:08:32 2020 -> Portable Executable support enabled.
   Sun Jun 28 19:08:32 2020 -> ELF support enabled.
   Sun Jun 28 19:08:32 2020 -> Mail files support enabled.
   Sun Jun 28 19:08:32 2020 -> OLE2 support enabled.
   Sun Jun 28 19:08:32 2020 -> PDF support enabled.
   Sun Jun 28 19:08:32 2020 -> SWF support enabled.
   Sun Jun 28 19:08:32 2020 -> HTML support enabled.
   Sun Jun 28 19:08:32 2020 -> XMLDOCS support enabled.
   Sun Jun 28 19:08:32 2020 -> HWP3 support enabled.
   Sun Jun 28 19:08:32 2020 -> Self checking every 3600 seconds.
   ```

6. Run a scan:
   ```
   sudo clamdscan –fdpass
   ```

   Response:
   ```
   /home/testuser: OK
   ----------- SCAN SUMMARY -----------
   Infected files: 0
   Time: 0.015 sec (0 m 0 s)
   ```

7. Test by downloading a virus file:
   ```
   wget www.eicar.org/download/eicar.com
   ```

8. Rescan:
   ```
   sudo clamdscan –fdpass
   ```

   Response:
   ```
   /home/ubuntu/eicar.com: Win.Test.EICAR_HDB-1 FOUND
   ----------- SCAN SUMMARY -----------
   Infected files: 1
   Time: 0.005 sec (0 m 0 s)
   ```

9. sudo mkdir /root/quarantine

10. Exclude certain directories from being scanned (all one line):
    ```
    sudo printf "ExcludePath ^/proc\nExcludePath ^/sys\nExcludePath
    ^/run\nExcludePath ^/dev\nExcludePath ^/snap\nExcludePath
    ^/var/lib/lxcfs/cgroup\nExcludePath ^/root/quarantine\n" | sudo
    tee -a /etc/clamav/clamd.conf
    ```

11. Restart clamav-daemon:
    ```
    sudo systemctl restart clamav-daemon
    ```

12. sudo su –

13. Execute clamdscan every night at 1:00 am (this is one continuous line):
    ```
    echo "0 1 * * * root /usr/bin/clamdscan --fdpass --
    log=/var/log/clamav/clamdscan.log --move=/root/quarantine /" |
    tee /etc/cron.d/clamdscan
    ```

14. Exit (from sudo su -)

15. Test full system scan (with quarantine file movement):
    ```
    sudo /usr/bin/clamdscan --fdpass --
    log=/var/log/clamav/clamdscan.log --move=/root/quarantine /
    ```

    Results:
    ```
    ---------------------------------------
    /snap: Excluded
    /run: Excluded
    /dev: Excluded
    /proc: Excluded
    /sys: Excluded
    /var/lib/lxcfs/cgroup: Excluded
    WARNING: /var/lib/lxd/unix.socket: Not supported file type
    /home/ubuntu/eicar.com: Win.Test.EICAR_HDB-1 FOUND
    /home/ubuntu/eicar.com: moved to ‘/root/quarantine/eicar.com’
    /root/quarantine: Excluded
    ----------- SCAN SUMMARY -----------
    Infected files: 1
    Total errors: 1
    Time: 235.497 sec (3 m 55 s)
    ```
16. Begin to enable real-time scanning:

```
sudo printf "OnAccessIncludePath /home\nOnAccessIncludePath
/var/www\nOnAccessExcludeUname clamav\nOnAccessExcludeRootUID
true" | sudo tee -a /etc/clamav/clamd.conf
```

17. Create a systemd file for clamonacc:

```
[Unit]
Description=ClamAV On Access Scanner
Requires=clamav-daemon.service
After=clamav-daemon.service syslog.target network.target

[Service]
Type=simple
User=root
ExecStartPre=/bin/bash -c "while [ ! -S /var/run/clamav/clamd.ctl
]; do sleep 1; done"
ExecStart=/usr/bin/clamonacc -F --config-
file=/etc/clamav/clamd.conf --log=/var/log/clamav/clamonacc.log -
-move=/root/quarantine

[Install]
WantedBy=multi-user.target
```

18. Enable and start the clamonacc daemon:

```
sudo systemctl enable clamonacc
sudo systemctl start clamonacc
```

19. Download a virus file to see if it's automatically detected and quarantined:

```
wget www.eicar.org/download/eicar.com
```

20. See if the file was moved:

```
ls -l
```

    Result:

```
Total: 0
```

21. Check the quarantine folder:

```
sudo ls /root/quarantine
```

    Result:

```
eicar.com
```

22. Check the logs:

```
sudo tail /var/log/clamav/clamonacc.log
```

    Result:

```
-------------------------------------
ClamInotif: watching '/home' (and all sub-directories)
ClamInotif: watching '/var/www' (and all sub-directories)
/home/testuser/eicar.com: Win.Test.EICAR_HDB-1 FOUND
/home/testuser/eicar.com: moved to '/root/quarantine/eicar.com'
```

MySQL Account Management Control Policy (NIST AC-2)

1. Create Roles and Create Users .

2. Assigned Roles to the Users.

3. The account will be automatically locked for a period of 1 day when the maximum number of unsuccessful logon attempts is exceeded.

MySQL Account Management Configuration (NIST AC-2)

1. Creating Users and roles :

```
CREATE ROLE manager;
CREATE ROLE readonly;
CREATE USER 'ge'@'localhost' IDENTIFIED BY 'MypPassword$123';
CREATE USER 'el'@'localhost' IDENTIFIED BY 'MyPassword$321';
```

Expected response for all the above:

```
Query OK, 0 rows affected (0.02 sec)
```

2. Granting roles access to database:

```
GRANT SELECT ON GroupProj.* to manager;
GRANT SHOW DATABASES on *.* to manager;
GRANT SELECT, INSERT, UPDATE, DELETE on GroupProj.* to manager;

GRANT SELECT ON GroupProj.* to readonly;
```

Expected response for all the above:

```
Query OK, 0 rows affected (0.02 sec)
```

3. Assigning the roles to the users:

```
GRANT manager TO 'el'@'localhost';
GRANT readonly TO 'ge'@'localhost';
```

Expected response for all the above:

```
Query OK, 0 rows affected (0.02 sec)
```

MySQL Separation of Duties Control Policy (NIST AC-5)

1. Have separate duties for each user .

2. Those users shouldn't be able to access other user stuff .

MySQL Separation of Duties Configuration (NIST AC-5)

Already have users and roles created from last nist-2 controls which are

1. USERS and Their Roles:

```
GRANT SELECT ON GroupProj.* to manager;
GRANT SHOW DATABASES on *.* to manager;
GRANT SELECT, INSERT, UPDATE, DELETE on GroupProj.* to manager;

GRANT SELECT ON GroupProj.* to readonly;
```

Expected response for all the above:

```
Query OK, 0 rows affected (0.02 sec)
```

2. Testing controls for manager:

```
Open sql terminal
Mysql –u el –p;
SET ROLE manager;
SELECT CURRENT_ROLE;
ADD TABLE TEST;
DROP TABLE TEST:
```

Expected response for all the above:

```
Query OK, 0 rows affected (0.02 sec)
```

3. Testing controls for manager:

```
Open sql terminal
Mysql –u el –p;
SET ROLE readonly;
SELECT CURRENT_ROLE;
ADD TABLE TEST;
```

Expected response for all the above:

```
Query OK, 0 rows affected (0.02 sec)
```

Got an error while adding the table TEST

ERROR 1044(42000): Acess denied for user ‘ge’@’localhost’
CREATE TABLE TEST denied in database ‘GroupProj’

MySQL System Use Control Policy (NIST AC-8)

1. Create or have some sort of Notification that will show the Usage

MySQL System Use Configuration (NIST AC-8)

1. In work Bench Go to Scripting
2. Go to scripting shell
3. Notification
4. Find notification of GroupProj

MySQL Role-Based Security Training Control Policy (NIST AT-3)

1. We don’t have any role based security training for our database.

2. In order to get that done the user should go through the policies made by the organization for their specific role.

3. The user should view all the training material.

4. The user should follow all the tools provided to make sure that the security is taken care of well.

MySQL Content of Audit Records Policy (NIST AU-3)

1. MySQL Audit records will be used to show the audits .

2. It will show the audits available under content of audit records.

3. Coordinates the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events.

MySQL Content of Audit Records Configure (NIST AU-3)

4. Copy audit_log.so to /usr/lib/mysql/plugin

5. In a connected and logged-in mysql prompt, run the following:
   ```
   install plugin audit_log soname 'audit_log.so';
   ```

   Expected response:
   ```
   Query OK, 0 rows affected (0.03 sec)
   ```

6. In a connected and logged-in mysql prompt, run the following:
   ```
   Show plugins;
   ```

   Expected response (near the bottom):
   ```
   | audit_log | ACTIVE | AUDIT | audit_log.so | GPL |
   46 rows in set (0.00 sec)
   ```

7. Add the below line to /etc/mysql/mysql.conf.d/mysql.cnf and save the file:
   ```
   audit_log_file = /var/log/mysql/audit.log
   ```

8. Restart MySQL:
   ```
   sudo systemctl restart mysql
   ```

9. In a connected and logged-in mysql prompt, run the following:
   ```
   mysql> show global variables like 'audit%';
   ```

   Expected result (or similar):
   ```
   +--------------------------+-------------------------+
   | Variable_name            | Value                   |
   +--------------------------+-------------------------+
   | audit_log_buffer_size    | 1048576                 |
   | audit_log_file           | /var/log/mysql/audit.log |
   | audit_log_flush          | OFF                     |
   | audit_log_format         | OLD                     |
   | audit_log_handler        | FILE                    |
   | audit_log_policy         | ALL                     |
   | audit_log_rotate_on_size | 0                       |
   | audit_log_rotations      | 0                       |
   | audit_log_strategy       | ASYNCHRONOUS            |
   ```

```
| audit_log_syslog_facility | LOG_USER                 |
| audit_log_syslog_ident    | percona-audit            |
| audit_log_syslog_priority | LOG_INFO                 |
+---------------------------+--------------------------+
12 rows in set (0.00 sec)
```

MySQL Time Stamp Control Policy (NIST AU-8)

1. Have some sort of time stamp on the data

2. We didn't had any time stamp on our tables so created one with time stamp.

MySQL Time Stamp Configuration (NIST AU-8)

1. Creating Table groupmemtitle tied to Groupmem so technically created two tables :

CREATE TABLE groupmemtitle(id INT PRIMARY KEY AUTO_INCREMENT, title varchar (300), content TEXT, publishdate DATETIME, expiredate DATETIME, updated TIMESTAMP default NOW() ON UPDATE NOW(), groupmem_id INT, FOREIGN KEY (groupmem_id) REFERENCES groupmem (id) ON DELETE NO ACTION) ENGINE = INNODB;

Expected response for all the above:

```
Query OK, 0 rows affected (0.02 sec)
```

2. Added data:

```
INSERT INTO groupmemtitle (title, groupmem_id) Values ('ODD',1);
INSERT INTO groupmemtitle (title, groupmem_id) Values ('PL',2);
INSERT INTO groupmemtitle (title, groupmem_id) Values
('PA/SR',4);
INSERT INTO groupmemtitle (title, groupmem_id) Values
('PA/SD',3);
INSERT INTO groupmemtitle (title, groupmem_id) Values
('PA/SC',5);
```

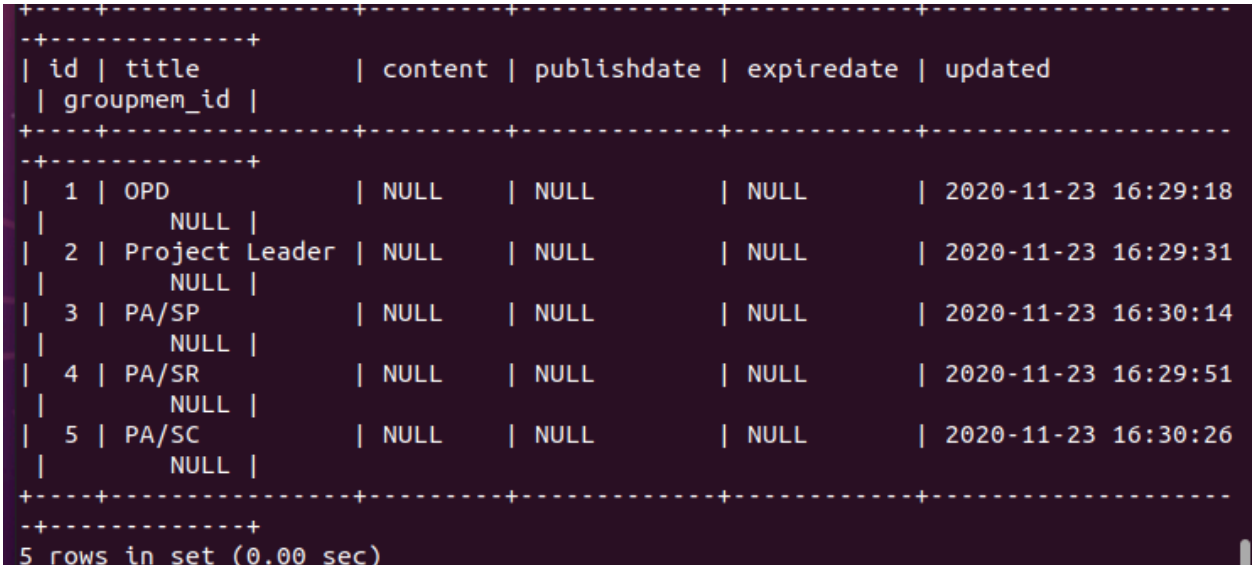
Expected response for all the above:

```
Query OK, 0 rows affected (0.02 sec)
```

3. Assigning the roles to the users:

```
SELECT * FROM groupmemtitle;
```

```
Shows the updated table
```



```
+----+----------------+---------+-------------+------------+---------------------
-+-------------+
| id | title          | content | publishdate | expiredate | updated
 | groupmem_id |
+----+----------------+---------+-------------+------------+---------------------
-+-------------+
|  1 | OPD            | NULL    | NULL        | NULL       | 2020-11-23 16:29:18
 |        NULL |
|  2 | Project Leader | NULL    | NULL        | NULL       | 2020-11-23 16:29:31
 |        NULL |
|  3 | PA/SP          | NULL    | NULL        | NULL       | 2020-11-23 16:30:14
 |        NULL |
|  4 | PA/SR          | NULL    | NULL        | NULL       | 2020-11-23 16:29:51
 |        NULL |
|  5 | PA/SC          | NULL    | NULL        | NULL       | 2020-11-23 16:30:26
 |        NULL |
+----+----------------+---------+-------------+------------+---------------------
-+-------------+
5 rows in set (0.00 sec)
```

MySQL Configuration Control Policy (NIST AT-3)

1. We don’t have any configuration control policy or change in this database.

2. If needed currently I am running this on a hard drive but can be moved to a secure measure like windows workbench or something else.

MySQL Fire Protection Control Policy (NIST PE-13)

1. Facilities need to maintain their server rooms, data centers, and mainframe computer rooms safe from fire.
2. Facilities will determine the best method to prevent Fire from damaging any of the equipment.

MySQL Fire Protection Configuration (NIST PE-13)

1. We don’t have any Fire Protection configuration.
2. If we needed to had one we will make sure that our area is equipped with best fire alarms, smoke detector and they are connected directly to 911 system.

Access Enforcement (NIST AC-3)

1. Information Systems should enforce approved authorizations for logical access to informations and system resources
2. Access enforcement can also be employed at the application level

MySQL Access Enforcement (NIST AC-3)

3. Login to mysql as root user which has full access `/usr/local/mysql/bin/mysql -u root -p`
4. Connect to database `use GroupProj;`
   Expected output: > Database changed
5. Attempt logical access to database `select City from Austria; delete from Austria where City = "Wels";`
   Expected output: > Query OK, 1 row affected (0.01 sec)

Permitted Actions Without Identification or Authentication (NIST AC-14)

1. Organization must specify what type of user actions can be performed on the information system without identification or authentication
2. Access is restricted for any user without authentication or identification on our system

MySQL Permitted Actions Without Identification or Authentication (NIST AC-14)

3. Open sql terminal
4. Create a user with not authentication `create user 'noAuth';`
   Expected output > Query OK, 0 rows affected (0.10 sec)
5. Try accessing the database `show databases;`
   Expected output >
```
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
4 rows in set (0.03 sec)
```
6. No access to the database ‘GroupProj’

Remote Access (NIST AC-17)

1. Organization established and documents user restrictions, connection requirements and implementation guidance for each type of remote access it allows
2. Organization authorize remote access prior to allowing connections

MySQL Remote Access (NIST AC-17)

3. Attempt remote access mysql -u root -h <host> -P 3306 -D GroupPorj -p

Publicly Accessible Content (AC-22)

1. Organization designated who can post information on publicly accessible information systems
2. Organization ensures that public information does not contain non public information
3. Organization reviews content before posting

MySQL Publicly Accessible Content (AC-22)

4. Create database from public information found at https://www.start.umd.edu/data-tools/global-terrorism-database-gtd
5. Connect to database as root user or any authorized user /usr/local/mysql/bin/mysql -u root -p
   use GroupProj;
   Expected output: > Database changed

6. Access public data select * from Brazil limit 5;
   Expected output: > 5 rows in set (0.01 sec)

Incident Handling (NIST IR-4)

1. Organization implements incident handling capabilities for security incidents
2. Organization uses lessons learned from ongoing incident handling to implement better incident response procedures, training and testing
3. Incident response capability is dependent on the capabilities of the information system
4. Incident related information can be obtained from a variety of sources including audit monitoring, network monitoring and administration reports

Incident Handling with MySQL Workbench (NIST IR-4)

5. Check some sources for incident handling by clicking “Server” on the toolbar
6. Click “Server Status” to see some incidents happening on the server. ex-CPU load, traffic, buffer usage
7. Click “Server logs” in order to see the log of incidents on server

System Development Life Cycle (NIST SA-3)

1. Organization manages the system using its own defined development life cycle that incorporated information security considerations
2. Organization defines and documents information security roles and responsibilities
3. Our system implements 4 roles in our development life cycle: database_administrator, end_user, client, testing
4. Each have their own responsibilities which we specified with the privileges granted: grant select, insert, update, delete / grant select, insert, update / grant select / grant select, update for database_administrator, end_user, client and testing respectively

Boundary Protection (NIST SC-7)

1. Information system monitors and controls communication at the external boundaries of the system
2. Information system implements subnetworks for publicly accessible components separated from internal networks
3. Information system only connects to external networks through managed interfaces consisting of boundary protection devices
4. Managed interfaces include gateways, routers, firewalls, guards or encrypted tunnels

Boundary Protection with MySQL Workbench (NIST SC-7)

5. On the toolbar click ‘Server’ then ‘Option files’ then “security” to view the boundary security on the server

Plan of Action and Milestones (NIST CA-5)

1. Organization develops a plan of action and milestones that they want to accomplish for remedial actions to correct weaknesses or deficiencies noted during the assessment of security controls.

2. With their current plan of actions and milestones, it should be constantly updated with findings from the assessments.

Baseline Configuration (NIST CM-2)

1. Organizations should create documents regarding the baseline configurations for each of its devices.

2. Software applications needed for the organizations should be downloaded onto the new devices and or pre-existing devices for the workstation.

3. Network Configurations should also be configured and set up on each device for the workstation

Baseline Configuration for MySQL Database (NIST CM-2)

1. Database/schema should be set up using one device utilizing MySQL Workbench

2. After creating database and importing all data, push to GitHub for other workstations to utilize “git pull” to receive the database

3. All workstations should pull the database onto the computer

4. Desktop or laptop device needs to Import data to MySQL Workbench and verify that it is working

Information System Backup (NIST CP-9)

1. Information Systems shall back up databases and any data within the database, but there is not documentation in need of backup. Any documentation should be stored in the same place.

2. Keep all of the backups of information in a safe place

3. With most updated changes to database, create a backup of database in MySQL Workbench

4. Conduct a backup by Clicking “Server” and then “Data Export”

5. Export all information needed to a selected dump folder, export the data, and then store in a secure storage location along with any existing documents.

Information System Recovery and Reconstitution (NIST CP-10)

1. With information systems crashing or losing any data/documentation, all data can be recovered from a created backup

2. Create a schema with title similar to data that was backed up

3. Click “Server” and then direct to “Data Import” option in drop down menu

4. Import data from selected folder by clicking the ellipses and locating the data from the most recent backup in storage location.

5. Select all data needed to be imported, and Click “Import Data”

6. Validate that all data has been imported and is usable by refreshing the Schema tab

Media Access (NIST MP-2)

1. For organizations, data any important data should be stored with flash drives, external hard drives, compact disks, etc., which is the digital method of storing data and important records

2. Non-digital method includes storing all important files, documentation, and records, in a storage area within the building

3. Access should be restricted so the development team only is able to access the data

Media Access with MySQL (NIST MP-2)

1. With the data present within' MySQL Workbench, click "Server" and then click "Data Export" from the drop-down menu.

2. Export the selected data into a dump folder in the designated file directory

3. Insert External Hard Drive or Flash Drive to device and transfer data over into external storage device.

4. Restrict access by placing a password lock on storage device; therefore, development team should only have access to data

Visitor Access Records (NIST PE-8)

1. Organizations should document all visitors that are accessing the building by recording entrance and departure times, date of access, identification, and purpose of visits.

2. Documentation can be digital or non-digital and stored for safe keeping

Visitor Access Records with MySQL Workbench (NIST PE-8)

1. Users accessing the database should record in a shared document of date access, identification, time accessed/time completed, and purpose for accessing database along with any changes created.

Water Damage Protection (NIST PE-15)

1. Facilities need to maintain a safe area for the server rooms, data centers, and mainframe computer rooms.

2. Facilities should file a request in regards to any water valves that are present within the server rooms, data centers, or mainframe computer rooms.

3. Facilities will determine the best method to prevent water valves from damage any of the equipment.

Use of External Information System Control Policy (NIST AC-20)

1. External information system should be able to access the organization's information system with authorization, and also able to process, store, or transmit organization-controlled information
2. The organization should restrict the use of organization-controlled portable storage devices by authorized individuals on external information system
3. The organization should prohibit the use of non-organizationally owned systems/components/devices

Security Training Record Control Policy (NIST AT-4)

1. The organization should document and monitor the system security training activities including basic security awareness training and specific security training.
2. The organization should retain the training records for a period based on the security policy.

User-Installed Software Control Policy (NIST CM-11)

1. The organization should establish governing the installation of software by users.
2. The organization needs to build alert system to enforce software installation policies.
3. The organization should monitor policy compliance regularly.

Incident Monitoring (NIST IR-5)

1. The organization tracks and documents information system security incidents

Incident Monitoring with MySQL Workbench (NIST IR-5)

1. Check some sources for incident monitoring by clicking “Server” on the toolbar
2. Click “Server logs” to see the error log files of the incidents on server
3. Click “Performance reports” in order to see incident related performance
4. Click “Users and Privileges” to see user information and privileges, in order to obtain incidents related info and user/administrator reports, also can monitor the physical access

Rules of Behavior (NIST PL-4)

1. The organization needs to establish rules that describe the responsibilities and expected behaviors with regard to information and information system usage for individuals who require access to the information system
2. The organization needs to document the agreements signed by such individuals
3. The organization should review and update the rules of behavior regularly
4. Individuals who have signed the agreements need to re-sign a copy if there is any update

Incident Monitoring with MySQL Workbench (NIST PL-4)

1. Check some sources for monitor individual users' behavior by clicking "Server" on the toolbar
2. Click "Performance reports" in order to see "User Resource Use"
3. Click "User Resource Use" to see "User Behavior Statistic Data"

Access Agreement (NIST PS-6)

1. The organization develops and documents access agreements for organizational information systems
2. The organization needs to review and update the access agreements regularly
3. The organization needs to ensure the user sign appropriate access agreements prior to being granted access
4. The organization needs to ensure the user re-sign the documents when the access agreements have been updated.

Access Agreement in MySQL Workbench (NIST PS-6)

1. Create database in MySQL Workbench from public information found at https://www.start.umd.edu/data-tools/global-terrorism-database-gtd
2. Open terminal and connect to database as root user or any user have the privilege to create roles.
   ~$ mysql -u root -p;.
   Then enter the password for root user.
   Expected output: able to connect to the database.
3. Use GroupProj database
   mysql> use GroupProj;
   Expected output: database changed
4. Create user role
   mysql> create role end_user;
   Expected output: role created
5. Create user 'GlobalProj_user' at localhost with password
   mysql> create user 'GlobalProj_user'@'localhost' identified by 'pA$sw0rD';
   Expected output: user created
6. After signing the access agreements, users will be granted access
7. Grant access and privileges for user role
   mysql> grant end_user to 'GlobalProj_user'@'localhost';
   mysql> grant select on GlobalProj.* to end_user;
   Expected output: role user gets the access and privileges

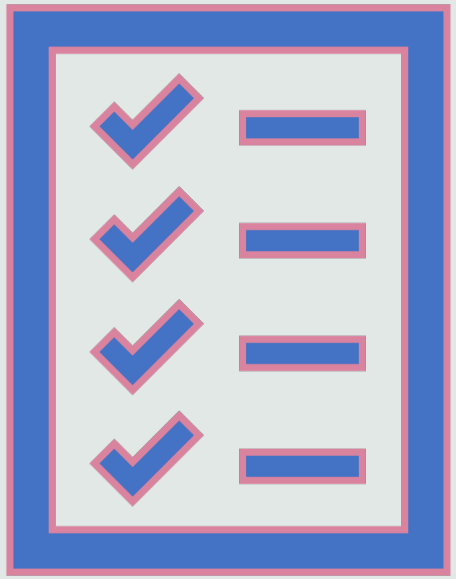
Third Party Personnel Security (NIST PS-7)

1. The organization establish personnel security requirements including security roles and responsibilities for third party providers
2. The organization requires third-party providers to comply with personnel security policies and procedures established by the organization
3. The organization should document personnel security requirements
4. The organization requires third-party providers to notify any personnel transfers or terminations of third-party personnel who have information system privileges.

Third Party Personnel Security in MySQL Workbench (NIST PS-7)

1. Create database in MySQL Workbench from public information found at https://www.start.umd.edu/data-tools/global-terrorism-database-gtd
2. Open terminal and connect to database as root user or any user have the privilege to create roles.
   ~$ mysql -u root -p;.
   Then enter the password for root user.
   Expected output: able to connect to the database.
3. Use GroupProj database
   mysql> use GroupProj;
   Expected output: database changed
4. Create client role
   mysql> create role client;
   Expected output: role created
5. Create user 'GlobalProj_client' at localhost with password
   mysql> create user 'GlobalProj_client'@'localhost' identified by 'pA$sw0rD';
   Expected output: user created
6. Grant access and privileges for client role
   mysql> grant client to 'GlobalProj_client'@'localhost';
   mysql> grant select on GlobalProj.* to client;
   Expected output: role client gets the access and privileges
7. After going through the personnel security policy and procedures and signing the agreements, third-party providers can get the access as client and should be able to use role client to connect to the database

Test Document



Items to be tested

Test Case #	Item to Test	Test Description	Test Date	Responsibility
1	AC-7	Unsuccessful Login Attempts	11/20/2020	Greg Eure
2	AU-2	Audit Events	11/20/2020	Greg Eure
3	CM-10	Software Usage Restrictions	11/21/2020	Greg Eure
4	IA-6	Authenticator Feedback	11/21/2020	Greg Eure
5	SA-2	Allocation of Resources	11/21/2020	Greg Eure
6	SC-5	Denial of Service Protection	11/21/2020	Greg Eure
7	SI-3	Malicious Code Protection	11/21/2020	Greg Eure
8	AC-2	Account Management	11/21/2020	Muhammad Zahid
9	AC-5	Separation of Duties	11/21/2020	Muhammad Zahid
10	AT-3	Role-Based Security Training	11/21/2020	Muhammad Zahid
11	AU-3	Content of Audit Records	11/21/2020	Muhammad Zahid
12	CM-6	Configuration Settings	11/22/2020	Muhammad Zahid
13	AU-8	Time Stamp	11/22/2020	Muhammad Zahid
14	AC-8	System Use Notification	11/22/2020	Muhammad Zahid
15	AC-14	Permitted Actions Without Identification or Authentication	11/22/2020	Estefania Lopez
16	AC-17	Remote Access	11/22/2020	Estefania Lopez
17	AC-22	Publicly Accessible Content	11/22/2020	Estefania Lopez
18	SA-3	System Development Life Cycle	11/25/2020	Estefania Lopez
19	IR-4	Incident Handling	11/23/2020	Estefania Lopez
20	SC-7	Boundary Protection	11/23/2020	Estefania Lopez
21	AC-3	Access Enforcement	11/23/2020	Estefania Lopez
22	PE-15	Water Damage Protection	11/23/2020	Calvin Ton
23	CA-5	Plan of Action and Milestones	11/23/2020	Calvin Ton
24	CP-9	Information System Backup	11/23/2020	Calvin Ton
25	CP-10	Information System Recovery and Reconstitution	11/23/2020	Calvin Ton
26	CM-2	Baseline Configuration	11/24/2020	Calvin Ton
27	MP-2	Media Access	11/24/2020	Calvin Ton
28	PE-8	Visitor Access Records	11/24/2020	Calvin Ton
29	AC-20	Use of External Information Systems	11/24/2020	Junyan Liu
30	AT-4	Security Training Record	11/24/2020	Junyan Liu
31	CM-11	User-Installed Software	11/24/2020	Junyan Liu
32	IR-5	Incident Monitoring	11/24/2020	Junyan Liu
33	PS-7	Third-Party Personnel Security	11/24/2020	Junyan Liu
34	PS-6	Access Agreements	11/24/2020	Junyan Liu
35	PL-4	Rules of Behavior	11/24/2020	Junyan Liu
36	PE-13	Fire Protection	11/25/2020	Muhammad Zahid

Test Approach(s)

Our testing approach was to follow the test case steps exactly, using the methods of INSPECT, TEST, OBSERVATION, and ANALYSIS, incorporate any test data, and then observe and document the results for each testing step. For any test cases where organizational document inspection was required, these were generally not available to be implemented.

Test Regulatory / Mandate Criteria

The system was tested using the 35 NIST 800-53 (Rev. 4) low-impact controls listed above

Test Pass / Fail Criteria

If the output of the command or step taken to test our database is as expected then we consider that a pass, if the output is not what we expected it is a fail.

Test Entry / Exit Criteria

Test case and any application and/or control documentation is available, and all prerequisite conditions are met. The exit criteria was different for every test but generally it was when we had enough data to pass the NIST control testing.

Test Deliverables

For each test we have filled out a form that includes the test case description, tester's name, date tested, prerequisties, steps, expected results, actual results, and whether the test passed, failed, was not executed, or was suspended.

Test Suspension / Resumption Criteria

Component testing will be suspended under the following conditions: critical error(s) found preventing test completion, change of business requirements, or change of environment components or technology including different version. Component testing will resume when the following criteria are met: all issues in suspension criteria have been resolved or mitigated.

Test Environmental / Staffing / Training Needs

In order to perform testing we needed to install a server running Ubuntu, install MySQL and MySQL Workbench, and import the GlobalProj database. Test users need to have a general understanding and proficiency with linux, and the mysql command-line, and limited understanding of MySQL Workbench.

Test Case ID	1	Test Case Description	Unsuccessful login attempts account lockout for 1 day after 3 invalid attempts		
Created By	Greg Eure	Reviewed By	Greg Eure	Version	1

QA Tester's Log	Test case passed

Tester's Name	Greg Eure	Date Tested	November 20, 2020	Test Case (Pass/Fail/Not	Pass

S #	Prerequisites:
1	Access to MySQL Server O/S via terminal or ssh
2	Account defined on O/S allowing remote login
3	Account defined on MySQL database server
4	Account configured for

S #	Test Data
1	userid = testuser
2	password = pAssw0rD

Test Scenario	Verify that account locks after entering wrong password 3 times

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	[TEST] Go to a command shell on the server where MySQL is installed.	Command shell should open	As expected	Pass
2	[TEST] Enter 'mysql -u testuser -p'	Should be prompted for password	As expected	Pass
3	[TEST] Enter an incorrect password	Access Denied	As expected	Pass
4	[TEST] Enter 'mysql -u testuser -p'	Should be prompted for password	As expected	Pass
5	[TEST] Enter an incorrect password	Access Denied	As expected	Pass
6	[TEST] Enter 'mysql -u testuser -p'	Should be prompted for password	As expected	Pass
7	[TEST] Enter an incorrect password	Access Denied; Account is blocked for 1 day due to 3 consecutive failed logins	As expected	Pass

Test Case ID	2	Test Case Description	Database access attempts cause event to be logged (auditing)		
Created By	Greg Eure	Reviewed By	Greg Eure	Version	1

QA Tester's Log	Test case passed

Tester's Name	Greg Eure	Date Tested	November 20, 2020	Test Case (Pass/Fail/Not	Pass

S #	Prerequisites:
1	Access to MySQL Server O/S via terminal or ssh
2	Account defined on O/S allowing remote login
3	Account defined on MySQL database server
4	MySQL Server configured according to NIST AU-2

S #	Test Data
1	userid = testuser
2	password = pAssw0rD

Test Scenario	Verify that audit is functioning and logging events

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	[TEST] Go to a command shell on the server where MySQL is installed.	Command shell should open	As expected	Pass
2	[TEST] Enter 'mysql -u testuser -p'	Should be prompted for password	As expected	Pass
3	[TEST] Enter 'use GroupProj;'	Database changed'	As expected	Pass
4	[TEST] Enter 'select * from GroupProj.Angola;'	7 rows in set (0.00 sec)	As expected	Pass

5	[TEST] Enter sudo cat /var/log/mysql/audit.log	<AUDIT_RECORD NAME="Query" RECORD="69_2020-11-21T01:59:59" TIMESTAMP="2020-11-21T02:12:05Z" COMMAND_CLASS="select" CONNECTION_ID="8" STATUS="0" SQLTEXT="select * from GroupProj.Angola" USER="root[root] @ localhost []" HOST="localhost" OS_USER="" IP="" DB="" />	As expected	Pass

Test Case ID	3	Test Case Description	Software inventory and peer-to-peer file sharing tracking		
Created By	Greg Eure	Reviewed By	Greg Eure	Version	1

OA Tester's Log	Test case passed

Tester's Name	Greg Eure	Date Tested	November 21, 2020	Test Case (Pass/Fail/Not	Pass

S #	Prerequisites:
1	Access to servers/systems where inventory audit
2	Software Inventory Docucment
3	Peer-to-Peer Tracking Document
4	

S #	Test Data
1	Software Inventory Docucment
2	Peer-to-Peer Tracking Document
3	
4	

Test Scenario	Verify all inventory tracking data is updated and accurate

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	[INSPECT] Compare Software Inventory with systems to be audited	Inventory should contain all software instance license as appropriate	As expected	Pass
2	[INSPECT] Compare Peer-to-Peer Tracking inventory with systems to be audited	Inventory should contain all peer-to-peer technology mappings as appropriate	As expected	Pass

Test Case ID	4	Test Case Description	Systems should not display authenticator feedback		
Created By	Greg Eure	Reviewed By	Greg Eure	Version	1

OA Tester's Log	Test case passed

Tester's Name	Greg Eure	Date Tested	November 21, 2020	Test Case (Pass/Fail/Not	Pass

S #	Prerequisites:
1	Access to system being tested
2	MySQL and MySQL Workbench installed
3	GroupProj database imported
4	MySQL server running

S #	Test Data
1	userid = testuser
2	password = pAssw0rD
3	
4	

Test Scenario	Verify that password isn't displayed on the screen as it's being typed

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	[TEST] Go to a command shell on the server where MySQL is installed.	Command shell should open	As expected	Pass
2	[TEST] Enter 'mysql -u testuser -p'	Should be prompted for password	As expected	Pass
3	[TEST] Enter password	password should not be displayed on screen when typed in	As expected	Pass
4	[TEST] Open MySQL Workbench	MySQL Workbench should open	As expected	Pass
5	[TEST] Open or create the connection to the local instance on port 3306	Logon dialog will display	As expected	Pass
6	[TEST] Enter user id and password	password should not be displayed on screen when typed in	As expected	Pass

Test Case ID	5	Test Case Description	Allocation of Resources		
Created By	Greg Eure	Reviewed By	Greg Eure	Version	1

OA Tester's Log	Test case not executed

Tester's Name	Greg Eure	Date Tested	November 21, 2020	Test Case (Pass/Fail/Not	Not Executed

S #	Prerequisites:
1	Access to budget and business planning
2	
3	
4	

S #	Test Data
1	
2	
3	
4	

Test Scenario	Review budget and planning documents to ensure compliance with NIST 800-53 item SA-2

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	[INSPECT] Inspect budget and business planning documents and ensure proper resources for information security are allocated.	Proper information security resources are allocated	There are no business planning documents	Not executed

Test Case ID	6	Test Case Description	Denial of Service Protection		
Created By	Greg Eure	Reviewed By	Greg Eure	Version	1

QA Tester's Log Test case not executed

Tester's Name	Greg Eure	Date Tested	November 21, 2020	Test Case (Pass/Fail/Not	Not Executed

S #	Prerequisites:
1	Access to firewalls and IPS
2	Access to network switches and routers
3	Access to network monitoring systems
4	Database is deployed in a clustered node

S #	Test Data
1	
2	
3	
4	

Test Scenario

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	[INSPECT] Look at firewall and IPS to ensure all avaiable DDoS configuration is enabled	DDoS configured is enabled	There are no firewall/IPS with DDoS protection	Not executed
2	[INSPECT] Look at switches and routers to ensure appropriate access lists are configured	ACLs are implemented with approprate rules that mitigate internal/external DDoS attacks	There are no switchs/routers with DDoS protection	Not executed
3	[INSPECT] Look at network monitoring to ensure monitoring controls and views are implemented to capture DDoS Alerts, and alerts are being monitored/acknowledged/escalated as appropriate	Monitoring alerts are configured and working for DDoS events	There is no network monitoring available	Not executed
4	[INSPECT] Confirm the database is deployed on clustered database nodes.	Database is deployed in a multi-node configuration	There is no multi-node configuration available	Not executed

Test Case ID	7	Test Case Description	Malicious Code Protection		
Created By	Greg Eure	Reviewed By	Greg Eure	Version	1

OA Tester's Log	Test case passed

Tester's Name	Greg Eure	Date Tested	November 21, 2020	Test Case (Pass/Fail/Not	Pass

S #	Prerequisites:
1	Access to system being tested
2	
3	
4	

S #	Test Data
1	userid = testuser
2	password = pAssw0rD
3	
4	

Test Scenario	Verify ClamAV is installed and running and quarantines malicious code

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	[TEST] Go to a command shell on the server where MySQL is installed.	Command shell should open	As expected	Pass
2	[TEST] tail /var/log/clamav/clamav.log	Sun Jun 28 19:08:32 2020 -> Portable Executable support enabled. Sun Jun 28 19:08:32 2020 -> ELF support enabled. Sun Jun 28 19:08:32 2020 -> Mail files support enabled. Sun Jun 28 19:08:32 2020 -> OLE2 support enabled. Sun Jun 28 19:08:32 2020 -> PDF support enabled. Sun Jun 28 19:08:32 2020 -> SWF support enabled. Sun Jun 28 19:08:32 2020 -> HTML support enabled. Sun Jun 28 19:08:32 2020 -> XMLDOCS support enabled. Sun Jun 28 19:08:32 2020 -> HWP3 support enabled. Sun Jun 28 19:08:32 2020 -> Self checking every 3600 seconds.	As expected	Pass

3	[TEST] wget www.eicar.org/download/eicar.com	1 file downloaded (eicar.com)	As expected	Pass
4	[TEST] ls -l eicar.com	no such file or directory	As expected	Pass
5	[TEST] sudo ls -l /root/quarantine	total 1 eicar.com	As expected	Pass
6	[TEST] sudo tail /var/log/clamav/clamonacc.log	---------- ClamInotif: watching '/home' (and all sub-directories) ClamInotif: watching '/var/www' (and all sub-directories) /home/testuser/eicar.com: Win.Test.EICAR_HDB-1 FOUND /home/testuser/eicar.com: moved to '/root/quarantine/eicar.com'	As expected	Pass

Test Case ID	8	Test Case Description	Account Management		
Created By	Muhammad	Reviewed By	Muhammad	Version	1

QA Tester's Log	Test Case Passed

Tester's Name	Muhammad	Date Tested	November 21, 2020	Test Case (Pass/Fail/Not	pass

S #	Prerequisites:
1	Accessed mySql through terminal
2	Created a Role with access to GropProj only
3	Created two users 'ge' and 'el'
4	Was able to log in and only access that database when logged under those users selecting other

S #	Test Data
1	user = ge , pass : MypPassword123
2	user = el , pass : MyPassword 321
3	
4	

Test Scenario	Given two users access to the database

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Accessed SQL through Terminal	Was able to access	As expected	Pass
2	Created a Role	The role got created	As expected	Pass
3	Created users and assigned them the role	User created and role assigned	As expected	Pass
4	Logged in using one account	Was able to log in	As expected	Pass
5	Accessed GroupProj	Access Given	As expected	Pass
6	Tried different database	Access Denied	As expected	Pass

Test Case ID	9	Test Case Description	Separation of Duties		
Created By	Muhammad	Reviewed By	Muhammad	Version	1

OA Tester's Log	Passed

Tester's Name	Muhammad	Date Tested	11/20/2020	Test Case (Pass/Fail/Not	Pass

S #	Prerequisites:
1	Deleted Roles from last test
2	Created New roles
3	Assigned roles
4	Test

S #	Test Data
1	user = ge , pass : MypPassword123
2	user = el , pass : MyPassword 321
3	
4	

Test Scenario	Verify if the duties thar are given are working

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Go to terminal and access SQL under root by mysql-u root -p	SQL should open for root	as expected	Pass
2	Created two roles by 'create role manager;' & 'create role acessonly;'	querry ok and role created	as expected	Pass
3	Assigned them to each user by grant role to -----	querry ok and role assigned	as expected	Pass
4	Granted manager to EL to manage the whole database GroupProj to manager by "Grant select on GroupProj.* to manager and show databases on *.* to manager"	no errors and it added the roles	as expected	Pass
5	Granted readonly to ge to read the whole database GroupProj to manager by "Grant connect any database to readonly and Grant select all user securable to readonly"	no errors and it added the roles	as expected	Pass
6	Tested by logging into mysql -u el -p	prompted for password	as expected	Pass
7	checked the role 'Select current_role();	should show manager role	as expected	Pass
8	Added and deleted a table	should add and delete	as expected	Pass

9	Tested by logging into mysql -u ge -p	prompted for password	as expected	Pass
10	checked the role 'Select current_role();	should show readonly role	as expected	Pass
11	Tried creating a new table	should give an error	as expected	Pass

Test Case ID	10	Test Case Description	Role-Based Security Training		
Created By	Muhammad	Reviewed By	Muhammad	Version	1

QA Tester's Log	No test case needed

Tester's Name	Muhammad	Date Tested	No test	Test Case (Pass/Fail/Not	No test case

S #	Prerequisites:
1	Access To the Policies
2	Access to the training material
3	Follow the procedures
4	Use tools provided

S #	Test Data
1	
2	
3	
4	

Test Scenario	Make sure users review the securit training

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
	The user needs to make sure that they reveiw the policies regarding the role	Should review the policies so they don't get into issues due to security	As Expected	No executed
	They should review the training material provided on the security of the role	should watch the training videos created for making sure they are secuired with their role	As Expected	No executed
	They should follow the procedures to do their role set by the companies	Don't share the information with other users	As Expected	No executed
	make sure they are using the tools provided for the security	Use Multi Authentication and don't save the password	As Expected	No executed

Test Case ID	11	Test Case Description	Content of Audit records		
Created By	Muhammad	Reviewed By	Muhammad	Version	1

QA Tester's Log Audit Records

Tester's Name	Muhammad	Date Tested	November 21, 2020	Test Case (Pass/Fail/Not	Pass

S #	Prerequisites:
1	Should have the sql terminal open
2	
3	
4	

S #	Test Data
1	user = el , pass : MyPassword 321
2	
3	
4	

Test Scenario

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
	Go to a command shell on the server where MySQL is installed.	Command shell should open	As expected	Pass
	Enter command 'mysql -u el -p'	Should be prompted for password	As expected	Pass
	Enter command 'set role manager'	should change the role	As expected	Pass
	[TEST] Enter 'use GroupProj;'	Database changed'	As expected	Pass
	Install Audit Log plugin	show install the audit plugin	As expected	Pass
	Restart and should show the audit records	Variable_name +---------- | audit_log_buffer_size | audit_log_file | audit_log_flush | audit_log_format | audit_log_handler | audit_log_policy | audit_log_rotate_on_size | audit_log_rotations | audit_log_strategy | audit_log_syslog_facility | audit_log_syslog_ident | audit_log_syslog_priority	As expected	Pass

Test Case ID	12	Test Case Description	Configuration Settings		
Created By	Muhammad	Reviewed By	Muhammad	Version	1

OA Tester's Log	Moving to a secure hardware

Tester's Name	Muhammad	Date Tested	November 2, 2020	Test Case (Pass/Fail/Not	Not executed

S #	Prerequisites:
1	Running workbench currently on an External
2	
3	
4	

S #	Test Data
1	
2	
3	
4	

Test Scenario	Moving to a secure hardware

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
	Moving it to a more secure os like mac or windows computer	Make sure proper security measures are added like microsoft authentication	Not implementing	Not executed

Test Case ID	13	Test Case Description	Time Stamp		
Created By	Muhammad	Reviewed By	Muhammad	Version	1

OA Tester's Log	Show time stamp

Tester's Name	Muhammad	Date Tested	November 22, 2020	Test Case (Pass/Fail/Not	Pass

S #	Prerequisites:
1	Get working SQL Workbench
2	Get a table to show time stamp
3	
4	

S #	Test Data
1	
2	
3	
4	

Test Scenario	Show time stamp

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Created a table group mem	Should have group mem info	as expected	Pass
2	created groupmemtitle and tied it with groupmem	title tied with groupmem	as expected	Pass
3	CREATE TABLE groupmemtitle(id INT PRIMARY KEY AUTO_INCREMENT, title varchar (300), content TEXT, publishdate DATETIME, expiredate DATETIME, updated TIMESTAMP default NOW() ON UPDATE NOW(), groupmem_id INT, FOREIGN KEY (groupmem_id) REFERENCES groupmem (id) ON DELETE NO ACTION) ENGINE = INNODB;	query went fine	as expected	Pass
4	Added data to the table	Timestamp should change	as expected	Pass

Test Case ID	14	Test Case Description	System Use Notification		
Created By	Muhammad	Reviewed By	Muhammad	Version	1

QA Tester's Log	Notifications of database

Tester's Name	Muhammad	Date Tested	November 22, 2020	Test Case (Pass/Fail/Not	Not executed

S #	Prerequisites:
1	
2	
3	
4	

S #	Test Data
1	
2	
3	
4	

Test Scenario	Find System notification

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Click Scripting	should show the scripting option	as expected	Pass
	Click scripting shell	should open the shell	as expected	Pass
	Go to Notification	should bring all the notification	as expected	Pass
	You will find all the notification	found the notification	as expected	Pass
	Add a Snipet for notification	will show system notification	as expected	Pass

Test Case ID	15	Test Case Description	Permitted Actions Without Identification or Authentication		
Created By	Estefania	Reviewed By	Estefania	Version	1

OA Tester's Log	Access without authentication or identification

Tester's Name	Estefania	Date Tested	November 22, 2020	Test Case (Pass/Fail/Not	pass

S #	Prerequisites:
1	Open sql terminal
2	create user with no authentication
3	
4	

S #	Test Data
1	/usr/local/mysql/bin/mysql -u root -p
2	create user 'noAuth';
3	
4	

Test Scenario	Try to access databse witout Authentication

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Try to access the database	No database will show, you need authentication to access db	as expected	Not executed

Test Case ID	16	Test Case Description	Remote Access		
Created By	Estefania	Reviewed By	Estefania	Version	1

OA Tester's Log Remote Access

Tester's Name	Estefania	Date Tested	November 22, 2020	Test Case (Pass/Fail/Not	not executed

S #	Prerequisites:
1	open sql terminal
2	
3	
4	

S #	Test Data
1	/usr/local/mysql/bin/mysql -u root -p
2	
3	
4	

Test Scenario Access databse remotely

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	try to access the database remotely	since we did not add a remote access feature, we should not be able to connect to the db remotely	as expected	not executed

Test Case ID	17	Test Case Description	Publicly Accessible Content		
Created By	Estefania	Reviewed By	Estefania	Version	1

OA Tester's Log Access Public Content

Tester's Name	Estefania	Date Tested	November 22, 2020	Test Case (Pass/Fail/Not	pass

S #	Prerequisites:
1	open sql terminal
2	Connect to GroupProj database
3	
4	

S #	Test Data
1	/usr/local/mysql/bin/mysql -u root -p
2	use GroupProj;
3	
4	

Test Scenario Access public content

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Access data from any table (select * from Brazil limit 5;)	5 rows in set (0.01 sec) -public data from Brazil table	as expected	pass

Test Case ID	18	Test Case Description	System Development Life Cycle		
Created By	Estefania	Reviewed By	Estefania	Version	1

OA Tester's Log System Development Life Cycle

Tester's Name	Estefania	Date Tested	November 25, 2020	Test Case (Pass/Fail/Not	Not executed

S #	Prerequisites:
1	define roles and responsibliies on database
2	
3	
4	

S #	Test Data
1	create role database_administrator; create role end_user; create role client; create role testing;
2	
3	
4	

Test Scenario Assess System Development Life Cycle

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	inspect our system development life cycle	Some implementation of security roles and resposibilities	As expected	Not executed

	19	**Test Case Description**	Incident Handling		
Created By	Estefania	**Reviewed By**	Estefania	**Version**	1

QA Tester's Log Incident Handling

Tester's Name	Estefania	**Date Tested**	November 23, 2020	**Test Case (Pass/Fail/Not**	not executed

S #	Prerequisites:
1	open mysql Workbech
2	
3	
4	

S #	Test Data
1	
2	
3	
4	

Test Scenario Accessing some Incident handling sources (ex. Server logs)

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	click server on the toolbar	report/log options show	as expeceted	not excuted
2	click server status	administrative server status including CPU load, InnoDB buffer usage, traffic, key efficiency, connections and many more	as expeceted	not excuted
3	click server logs	server logs are available to show incidents on server	as expeceted	not excuted
4	click option files	server confiugrations are available to change, including general, advanced and	as expeceted	not excuted

Test Case ID	20	Test Case Description	Boundary Protection		
Created By	Estefania	Reviewed By	Estefania	Version	1

OA Tester's Log	Chech Boundary Protection

Tester's Name	Estefania	Date Tested	November 23, 2020	Test Case (Pass/Fail/Not	not executed

S #	Prerequisites:
1	open sql workbench
2	
3	
4	

S #	Test Data
1	
2	
3	
4	

Test Scenario	Check Boundary Protection

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	click server in toolbar	several server view options	as expected	not executed
2	click option files	server configurations	as expected	not executed
	click security	boundary security configurations	as expected	not executed

Test Case ID	21	Test Case Description	Access Enforcement		
Created By	Estefania	Reviewed By	Estefania	Version	1

OA Tester's Log Access Enforcement

Tester's Name	Estefania	Date Tested	November 23, 2020	Test Case (Pass/Fail/Not	pass

S #	Prerequisites:
1	open sql terminal
2	
3	
4	

S #	Test Data
1	/usr/local/mysql/bin/mysql -u root -p
2	
3	
4	

Test Scenario Access database as authorized user

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	login as root user	access to groupProj database	as expected	pass
2	switch to GroupProj database	Database changed	as expected	pass
	select City from Austria;	list of city in Austria table	as expected	pass
	edit table - delete from Austria where City = "Wels";	Query OK, 1 row affected (0.01 sec)	as expected	pass

Test Case ID	22	Test Case Description	Water Damage Protection		
Created By	Calvin Ton	Reviewed By	Calvin Ton	Version	1

OA Tester's Log	Test case not executed

Tester's Name	Calvin Ton	Date Tested	November 23rd, 2020	Test Case (Pass/Fail/Not	Not Executed

S #	Prerequisites:
1	Access Server Room/Data Center
2	
3	
4	

S #	Test Data
1	
2	
3	
4	

Test Scenario	Verify that server room is protected from water

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Inspect area and make sure isolation values are employed to shut off water supply	Shut off water valves in server rooms, data centers, and mainframe computer rooms	No server room, datacenter, or mainframe computer room to protect from water	Not Executed

Test Case ID	23	Test Case Description	Plan of Action and Milestones		
Created By	Calvin Ton	Reviewed By	Calvin Ton	Version	1

OA Tester's Log	Test Case not executed

Tester's Name	Calvin Ton	Date Tested	Novemeber 24th, 2020	Test Case (Pass/Fail/Not	Not Executed

S #	Prerequisites:
1	Access to Word Document
2	
3	
4	

S #	Test Data
1	
2	
3	
4	

Test Scenario	Verify that ogranization has plan of action and milestones to accomplish

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Develop plan of action and milestones for information system to document the organization's planned remedial action to correct weaknesses or deficiencies	Proper plans of actions along with milestone for future	No plan of action or milestones were created	Not executed

Test Case ID	24	Test Case Description	Information System Back up		
Created By	Calvin	Reviewed By	Calvin	Version	1

OA Tester's Log	Test case passed

Tester's Name	Calvin	Date Tested	November 23rd, 2020	Test Case (Pass/Fail/Not	Pass

S #	Prerequisites:
1	Download MySQL Workbnech
2	Be able to Log into Root
3	
4	

S #	Test Data
1	Log into root of LocalHost
2	
3	
4	

Test Scenario	Verify that data is backed up and stored in a secure location

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Type mysql-workbench into linux terminal	MySQL Workbench opens	As expected	Pass
2	Create a Schema and Create the tables	Schema created along with tables imported with data	As expected	Pass
3	Click"Server" Tab	Drop down menu opens	As expected	Pass
4	Click "Data Export"	Brings user to Data Export page to back up data	As expected	Pass
5	Select Schema and tables to Back up	Schema is Checked and all tables in Schema are "checkmarked"	As expected	Pass
6	Click "Start Export"	Data Exports into a dump folder	As expected	Pass

Test Case ID	25	Test Case Description	Information System REcovery and Reconstitution		
Created By	Calvin	Reviewed By	Calvin	Version	1

QA Tester's Log	Test Case Passed

Tester's Name	Calvin	Date Tested	November 23rd, 2020	Test Case (Pass/Fail/Not	Pass

S #	Prerequisites:
1	Access to Files
2	Access to working MySQL Workbnech
3	
4	

S #	Test Data
1	Log into root of LocalHost
2	
3	
4	

Test Scenario	Verify that data is recovered and is useable

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Type mysql-workbench into linux terminal	MySQL Workbench opens	As expected	Pass
2	Create Schema ready for data import and refresh tab	Created Schema appears on left tab	As expected	Pass
3	Click "Server" and then "Data Import"	Drop down menu opens and "Data Import" option available. Data Import page opens.	As expected	Pass
4	Select elipses after the "Import from Dump Project Folder" and select the correct backup dump folder	File application opens and all dump folder options available	As expected	Pass
5	Select Imported Schema and make sure all tables are selected	Checkmarks are next to Schema and Tables	As expected	Pass
6	Click "Start Import"	Data Imported into MySQL Workbench as well as mysql in terminal	As expected	Pass

Test Case ID	26	Test Case Description	Baseline Configuration		
Created By	Calvin	Reviewed By	Calvin	Version	1

OA Tester's Log	Test case attempted

Tester's Name	Calvin	Date Tested	November 24th, 2020	Test Case (Pass/Fail/Not	Not Executed

S #	Prerequisites:
1	Access to Documentation
2	
3	
4	

S #	Test Data
1	
2	
3	
4	

Test Scenario	Verify that organization has a baseline documentation

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Open a Google Document or Word Document	Google Doc opens/Word Document Opens	As expected	Pass
2	Document a base setup for the organization's system/data	Document Should be filled with base where companh sets up devices and data	There was nothing to document as a baseline	Not Executed

Test Case ID	27	Test Case Description	Media Access		
Created By	Calvin	Reviewed By	Calvin	Version	1

OA Tester's Log	Test Case Passed

Tester's Name	Calvin	Date Tested	November 24th, 2020	Test Case (Pass/Fail/Not	Pass

S #	Prerequisites:
1	Access to Sotraage device i.e Flash Drive
2	
3	
4	

S #	Test Data
1	
2	
3	
4	

Test Scenario	Verify that external storage device stores data and is secured

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Click "Server" and then click "Data Export"	Takes user to Data export page	As expected	Pass
2	Select dump folder to store data in and click "Start export"	Data should export into a dump folder in the selected directory	As expected	Pass
3	Insert Flash Drive/External Hard Drive into Device	Device should recognize Flash Drive/External Hard drive	As expeced	Pass
4	Copy dump folder over to Flash Drive storage	Dump folder should appear in Flash Drive directory	As expected	Pass
5	Lock so=torage device with a password	Storage should not be able to be accessible unless password is provided	As expected	Pass

Test Case ID	28	Test Case Description	Visitor Access Records		
Created By	Calvin	Reviewed By	Calvin	Version	1

OA Tester's Log	Test case not executed

Tester's Name	Calvin	Date Tested	November 24th, 2020	Test Case (Pass/Fail/Not	Not Executed

S #	Prerequisites:
1	Access to documentation software
2	
3	
4	

S #	Test Data
1	
2	
3	
4	

Test Scenario	Verify that visitors and users are being documented when accessing building or data

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Document when users or visitors access data within database	Record is recorded	No documentation created as everything done remotely	Not expected

Test Case ID	29	Test Case Description	Use of external information systems		
Created By	Junyan	Reviewed By	Junyan	Version	1

OA Tester's Log	Test Case Passed

Tester's Name	Junyan	Date Tested	November 24th, 2020	Test Case (Pass/Fail/Not	Pass

S #	Prerequisites:
1	Use command line to log into mysql
2	
3	
4	

S #	Test Data
1	~$ mysql -u GlobalProj_admin -p
2	
3	
4	

Test Scenario	Verify acccess the information system from external information without authorized password will be denied

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Try to access the dtabase as an external information system	Access denied due to no authorized password	as expected	Not executed

Test Case ID	30	Test Case Description	Security Training Records		
Created By	Junyan	Reviewed By	Junyan	Version	1

OA Tester's Log	No test case needed

Tester's Name	Junyan	Date Tested	No test	Test Case (Pass/Fail/Not	No test case

S #	Prerequisites:
1	Access to the training documents
2	Follow the procedures
3	
4	

S #	Test Data
1	
2	
3	
4	

Test Scenario	make sure all the training records are documented and monitored

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
	Organization documents and monitors users' security training activities including basic security awareness training and specific security training	Training records are documented and monitored	As Expected	No executed
	Organization retains the training records for a time period based on the security policy	Training records are retained in a specific period	As Expected	No executed

Test Case ID	31	Test Case Description	User Installed Software		
Created By	Junyan	Reviewed By	Junyan	Version	1

OA Tester's Log	Test case passed

Tester's Name	Junyan	Date Tested	November 24th, 2020	Test Case (Pass/Fail/Not	Pass

S #	Prerequisites:
1	Software Installation auditing tools
2	Software installation policies
3	
4	

S #	Test Data
1	Software installation policies
2	
3	
4	

Test Scenario	User has the ability to install software with necessary privilege; unauthorized installation will trigger system alert

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Establish governing the installation of software by users	Users have the ability to install software with necessary privileges	As expected	Pass
2	Enforce software installation policies through alarming system	alerts should be sent out for unauthorized installations	As expected	Pass

Test Case ID	32	Test Case Description	Incident Monitoring		
Created By	Junyan	Reviewed By	Junyan	Version	1

QA Tester's Log	Test Case Passed

Tester's Name	Junyan	Date Tested	November 24th, 2020	Test Case (Pass/Fail/Not	not executed

S #	Prerequisites:
1	open MySQL Workbench
2	
3	
4	

S #	Test Data
1	Servers Log
2	Performance reports
3	Users info
4	Privilege info

Test Scenario	Use MySQL workbench to monitor system incidents

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	click Server on the toolbar	Server logs, Performance reports and other options are available	as expeceted	not excuted
2	click Server logs	Error log files are available to show server errors	as expeceted	not excuted
3	click Performance reports	Performance reports including memory usage,database schema statistics, wait event times are showing up	as expeceted	not excuted
4	click Users and Privileges	pysical access like Users and privileges info is available	as expeceted	not excuted

Test Case ID	33	Test Case Description	Third-Party Personnel Security		
Created By	Junyan	Reviewed By	Junyan	Version	1

OA Tester's Log	Test Case Passed

Tester's Name	Junyan	Date Tested	November 24th, 2020	Test Case (Pass/Fail/Not	Pass

S #	Prerequisites:
1	personnel security policies and procedures
2	personnel security requirements
3	
4	

S #	Test Data
1	create role client;
2	create user 'GlobalProj_client'@'localhost' identified by 'pA$sw0rD';
3	grant client to 'GlobalProj_client'@'localhost';
4	grant select on GlobalProj.* to client;

Test Scenario	Third party with authorized role has the ability to log in to the system

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	create role client; create user 'GlobalProj_client'@'localhost' identified by 'pA$sw0rD';	client role is created with password	as expeceted	pass
2	grant client to 'GlobalProj_client'@'localhost'; grant select on GlobalProj.* to client;	grant client role the access to the database	as expeceted	pass
3	third party uses the user name and password to log into the database	Third party logs into the database successfully	as expeceted	pass

Test Case ID	34	Test Case Description	Access Agreements		
Created By	Junyan	Reviewed By	Junyan	Version	1

OA Tester's Log	Test Case Passed

Tester's Name	Junyan	Date Tested	November 24th, 2020	Test Case (Pass/Fail/Not	Pass

S #	Prerequisites:
1	Access Agreements
2	use command line to create database user
3	
4	

S #	Test Data
1	create role end_user;
2	create user 'GlobalProj_user'@'localhost' identified by 'pA$sw0rD';
3	grant end_user to 'GlobalProj_user'@'localhost';
4	grant select, insert, update on GlobalProj.* to end_user;

Test Scenario	User who signed the access agreements has the authorized role and is able to log into the system

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	create role end_user; create user 'GlobalProj_user'@'localhost' identified by 'pA$sw0rD';	user role is created with password	as expeceted	pass
2	grant end_user to 'GlobalProj_user'@'localhost'; grant select, insert, update on GlobalProj.* to end_user;	grant user role the access to the database	as expeceted	pass
3	user uses the user name and password to log into the database	user logs into the database successfully	as expeceted	pass

Test Case ID	35	Test Case Description	Rules of Behavior		
Created By	Junyan	Reviewed By	Junyan	Version	1

OA Tester's Log	Test Case Passed

Tester's Name	Junyan	Date Tested	November 24th, 2020	Test Case (Pass/Fail/Not	Not executed

S #	Prerequisites:
1	Open MySQL workbench
2	
3	
4	

S #	Test Data
1	User Resource Use
2	User behavior statistic data
3	
4	

Test Scenario	Use MySQL workbench to monitor user behaviors

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	click Server on the toolbar	Performance reports option is available	as expeceted	not excuted
2	click Performance reports	User Resource Use option is available	as expeceted	not excuted
3	click User Resource Use	User behaviors statistic data are available	as expeceted	not excuted

Test Case ID	36	Test Case Description	Fire Protection		
Created By	Muhammad	Reviewed By	Muhammad	Version	1

OA Tester's Log	Test case not executed

Tester's Name	Muhammad	Date Tested	11/25/2020	Test Case (Pass/Fail/Not	Not Executed

S #	Prerequisites:
1	Access Server Room/Data Center
2	
3	
4	

S #	Test Data
1	
2	
3	
4	

Test Scenario	Verify that server room is protected from water

Step #	Step Details	Expected Results	Actual Results	Pass / Fail / Not executed / Suspended
1	Doesn't Apply to us but if it did we will implement fire hazard detection devices to catch up on incident if anything occur	Have fire alarms and smoke alarms in server rooms, data centers, and mainframe computer rooms connected to	No server room, datacenter, or mainframe computer room to protect from Fire	Not Executed