11. Training

**AT-4 Training Records**

Literacy training and awareness is a good practice for improving the security of any system. Users at every level and position should receive adequate training. Users can be defined as employees or contractors that work requires connecting to the system. Users can also be categorized by the roles and the scope of access they have. They can have direct or indirect access to databases and other parts of the system. With direct access, they might have different roles within the system, with indirect access they might have access to the building or server room where the system is stored. Some of the departments or contractors can have partial access to the system or its components like the network that servers are connected to (e.g., IT Maintenance Department) or information about users (HR Department) or the company (CEO, CFO, etc.). Hence, it is crucial to be aware that cyberattacks can have different forms (phishing, pharming, whaling, website spoofing, social engineering, mining, etc.) and can eventually lead to the unauthorized breach of the system.

Training is one of the techniques that can prevent unwanted attacks. The scope of users’ preparation should include general security training and more specific role/position training. To provide maximum security, all pieces of training should be described in-depth under the AT-2 and AT-3 controls specifications and the records of that training should be kept under the AT-4 control specification.

AT-4 is a control for security practice where the records of all users’ training and certification are kept. Especially, the documentation should include education, training, and certification requirements for each type of user. Also, there should be records of each user’s completion of those requirements.

The records can be held in tabular form and managed by HR Department. The specifications for Training Records Database tables can be following:

1. Roles
   1. Specification (Unique ID)
   2. Title
   3. Description
2. Controls
   1. Specification (Unique ID)
   2. Title
   3. Access Scope
   4. Description
3. Certifications
   1. Certification ID
   2. Certification Name
   3. Certification Provider
   4. Certification Description
4. Users Records
   1. User ID
   2. User Name
   3. User Last Name
   4. User date of hiring
   5. User Role
5. Template
   1. Report ID
   2. User ID
   3. Role ID
   4. Certification ID
   5. Date of Completion
   6. Report Date

**Storage of the database**

AT-4 Controller specifically regards records of the certification and keeps them up to date. Therefore, the simple documentation in Microsoft Access can be made and managed by HR. As well, it can be stored as a database file on the institution’s server and updated by the DB manager.

**Access to the database**

Documentation in MS Access can be accessed by the HR manager anytime as it is needed. Yet the database on the server should be accessed only by users who are granted access to the part of the server where the database is located. Database on the server should include more detailed information about employees and certifications, therefore, it should not have general access. With general access, there is a risk of social engineering attacks. Perhaps, an unauthorized person can determine who exactly they should approach to obtain needed credentials.

**Updates to the database**

The databases should be updated regularly and according to policies defined by the company. To keep consistency, the .csv file of all records can be kept as a backup and used to transfer records between the server database (managed by DB Manager) and MS Access (managed by HR manager).

**Tables Description**

1. Roles

It contains information about specific roles given to users of the database system. There are different functions and clearance of different roles, therefore, the Roles table’s purpose is to store them all. The table has organizational purposes so it should include a uniquely assigned ID (primary key), title, and a brief description.

1. Controls

The purpose of the Controls table is to store all controls used in the system. That table is also organizational in nature, so it is not needed to include detailed information about the controller, just the main attributes. The table should have columns like ID (primary key), title, role’s manager, and a brief description. That practice can also prevent obtaining detailed information about databases by unauthorized users.

1. Certifications

The Certifications table, similarly, should contain basic information about the required certifications, which should have been obtained by the user before beginning working on the database. For record purposes, the table should include columns like certification ID (primary key), its name, provider, and a brief description.

1. Users

Users table is the record of all employees. Each attribute in the database should have a unique ID (primary key), first and last name of the user, their start date, role ID. That table specifies each employee’s role and the date of hiring, which helps in determining which certification and by when should be completed.

1. Template Example

The Template table is an example of how the records of the training can be stored. It is an example because different types of training records might be required for different database systems. Also, the specification of the records should be defined in the system or institution policy. The sample template is prepared accordingly to the policy stating that training records should include the user ID, user role, certifications required by the role, and the dates when they were completed. The table can be easily modified. It can be extended with columns like proof of certification (e.g., pdf file, image) released by the certification provider. It can be adjusted for the specific roles or controllers, not users. For documentation purposes, it is recommended to include the date of added record.

Based on the Template table, the general and cumulative report of the records can be created. It can be easily done in MS Access or in SQL software.

**Certifications Requirements**

Specification of required certifications should be included in the system or institution’s policies. Also, those specifications should be mirrored in the databases up to date.

CompTia A+

The certification provides general knowledge about security systems. It shows that the user has basic knowledge about hardware, OS, software troubleshooting, networking, security, etc. It is required for the Database Designer role.

Google IT Cert

The certification provides the knowledge for basic system operations. It is required for most of the employees in the IT department. In the database system, it is required for Database Designers and Basic Users.

CompTia Security+

The certification validates an applicant’s skills in cybersecurity. It is required for all users with at least medium access to the system. The certification is compliant with ISO 17024 standards and approved by US DoD. It is required for Database Managers.

CISSP

Certified Information Systems Security Professional is a certification that proves users’ skills in design, implementation, and management of the security in the databases systems. It is required for Database Administrators.

CISM

ISACA’s Certified Information Security Manager is for users with advanced knowledge of IT security. It is required for Database Administrators.

SSCP

Systems Security Certified Practitioner is a certification implementing security administration and its management. It provides knowledge of the best security practices in IT infrastructure, policies and procedures’ creation and administration. It is required for Database Managers.

Policy Training

Policy training is on-site training prepared by HR management and the IT department. The purpose of the training is to increase awareness of all employees. The security of the system depends not only on users with access to the server but also on front-end users, contractors, or even maintenance staff working around the servers. Therefore, all employees should receive general training and be provided with any general updates and changes to the security policies. The training should include all kinds of employees and should be sectioned accordingly, so every employee is aware of risk within their roles and can receive an appropriate education.

**Summary**

Security Training is crucial in keeping the system safe. Database systems can vary in size, purposes, the significance of the stored records, etc. Thus, the knowledge and skills of the database’s users make it venerable. To make sure the users are prepared to work on the database, the system of reporting the training must be developed. The controller AT-4 is an example of a database component assuring that records of the training are constantly updated. It can be done in tabular form with tables storing information about required certification, courses, or other related training as well as information about the database’s roles, controllers, users. Also, there can be various places where the tables can be stored. They can be located on the hard drive or the cloud as an MS Access file or they can be turned into a database and stored as SQL file on the server. The MS Access file can serve a purpose for records documentation at the HR department. The SQL file on the server can be a documentation form for the database and its users. Regardless of the location of the file, both can be identical, or they can have different specifications. Yet, it is important to adjust the access to the file accordingly to the sensitivity of the information included in each file. Without proper information protection, cyberattacks in different forms can happen. Therefore, awareness is so important. Cybersecurity literacy is an effective technique to increase that awareness and deliver needed skills to build proper protection for the system. It is also crucial to have adequate documentations of the training and certification so it can be easily shown that the security management is well-developed and up to date.